INTEGRATED CIRCUIT WEAR-OUT PREDICTION AND RECYCLING DETECTION USING RADIO-FREQUENCY DISTINCT NATIVE ATTRIBUTE FEATURES

DISSERTATION

Randall D. Deppensmith, Lt Col, USAF

AFIT-ENG-DS-16-D-002

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this document are those of the author and do not reflect the official policy or position of the United States Air Force, the United States Department of Defense or the United States Government.

AFIT-ENG-DS-16-D-002

INTEGRATED CIRCUIT WEAR-OUT PREDICTION AND RECYCLING DETECTION USING RADIO-FREQUENCY DISTINCT NATIVE ATTRIBUTE FEATURES

DISSERTATION

Presented to the Faculty
Graduate School of Engineering and Management
Air Force Institute of Technology
Air University
Air Education and Training Command
in Partial Fulfillment of the Requirements for the
Degree of Doctor of Philosophy

Randall D. Deppensmith, B.S.E.E., M.S.E.E.
Lt Col, USAF

December 2016

AFIT-ENG-DS-16-D-002

INTEGRATED CIRCUIT WEAR-OUT PREDICTION AND RECYCLING DETECTION USING RADIO-FREQUENCY DISTINCT NATIVE ATTRIBUTE FEATURES

DISSERTATION

Randall D. Deppensmith, B.S.E.E., M.S.E.E.
Lt Col, USAF

Committee Membership:

Michael A. Temple, PhD
Chairman

Samuel J. Stone, Maj, USAF, PhD
Member

Matthew C. Fickus, PhD
Member

ADEDJI B. BADIRU, PhD
Dean, Graduate School of Engineering and Management

AFIT-ENG-DS-16-D-002

Abstract

Radio Frequency Distinct Native Attributes (RF-DNA) have shown promise for detecting differences in Integrated Circuit (IC) devices using statistical features extracted from device side channel Unintentional Radio Emissions (URE). Such capability has been leveraged to support physical layer cyber-security applications by identifying altered components, detecting Trojan hardware, and detecting un-authorized software configurations. The hardware discrimination ability of RF-DNA relies upon the unique process variation imparted to a semiconductor device during manufacturing. However, the internal components (transistors, etc.) in modern IC devices do not maintain consistent performance characteristics as they electronically age and wear out over their operational lifetime. The effects of wear-out include alteration of a devices URE and potential changes in RF-DNA feature discriminability. If sufficient age-dependent change occurs and is captured in time varying RF-DNA features the device age may be predicted without dedicated in-situ sub-circuits. Additionally, existing cyber-security applications may lose accuracy. This work addresses device age characterization by accelerating device wear-out using an experimental high temperature cycling approach and 16 Texas Instruments MSP430 micro-controller ICs. RF-DNA techniques are adopted from prior work and applied to MSP430 URE to address the following research goals: 1) How does device wear-out impact RF-DNA features and device age discriminability? 2) Can device age be continuously estimated by monitoring time varying changes in RF-DNA features? 3) Can device age state (e.g., new vs. used) be reliably estimated? Research conclusions include: 1) device wear-out does impact RF-DNA features, with up to a 16% change in discriminability demonstrated for the range of accelerated ages considered, 2) continuous (hour-by-hour) age estimation for failure prediction was most challenging and generally not supported, and 3) binary new vs. used age estimation for counterfeit recycled device detection was successful with 78.7% to 99.9% average discriminability achieved for all device-age combinations considered.

Dedication

I am extremely grateful for my wonderful family. You have been amazing dealing with my crazy schedule, late nights and in the last weeks of my efforts juggling my stress and the needs of our new baby. Linus and Hadley, thank you for always giving me smiles, happy tail wags and greeting me with excited barks and hugs no mater if I returned home happy or frustrated.

Col Butler, Col Clark and the entire USAF Academy Department of Electrical and Computer Engineering, thank you for placing your faith in my ability, and offering the pipeline opportunity. I am excited to get back to USAFA and teach the cadets again.

Finally, thanks to the Lord Jesus Christ who has blessed me with all that I have. Without your grace nothing I attempt matters.

Let us not become weary in doing good, for at the proper time we will reap a harvest if we do not give up – Galatians 6:9

Acknowledgements

I would like to thank Dr. Mary Lanzerrotti for helping me start this journey and refining the focus of my PhD research. Dr. Michael Temple and Maj Samuel Stone thank you for swapping committee chair rolls as deployments and life event timing dictated adapting the completion plan. I owe many thanks to all the committee members (Maj Stone, Dr. Temple, Dr. Fickus) for keeping me focused and providing guidance along the way when original efforts did not work the way I had hoped.

To my fellow RF-DNA PhD students (John Rice and Matthew Lukacs), thanks for being willing to listen to my frustrations and bouncing ideas between our collective research efforts. These discussions helped more than you know.

Randall D. Deppensmith

Table of Contents

Page

Page

List of Figures

Figure Page

Figure Page

Figure Page

List of Tables

List of Abbreviations

AES Advanced Encryption Standard 52

AFIT Air Force Institute of Technology 12

ASIC Application Specific Integrated Circuit 28

AWGN Additive White Gaussian Noise 18

BPF Band Pass Filter 51

BTI Bias Temperature Instability 3

CDF Cumulative Distribution Function 75

CMOS Complementary Metal Oxide Semiconductor 28

CMY Cyan-Magenta-Yellow 70

DC Direct Current 38

DoD Department of Defense 2

DSP Digital Signal Processing 14

DUT Device Under Test 6

EER Equal Error Rate 26

EM Electromagnetic 16

EMC	Electromagnetic Compatibility	31
EMI	Electromagnetic Interference	31
FET	Field Effect Transistor	3
fF	femto Farad	40
FFT	Fast Fourier Transform	63
FO-4	Fan Out 4	40
FPGA	Field Programmable Gate Array	28
FVR	False Verification Rate	24
GHz	Giga-Hertz	16
GRLVQI	Generalized Relevance Learning Vector Quantization Improved	16
GSps	Giga-Samples per second	16
HC	Hot Carrier	36
HTOL	High Temperature Operating Life	55
IC	Integrated Circuit	7
LED	Light Emitting Diode	105
LPF	Low Pass Filter	16

MDA/ML Multiple Discriminate Analysis / Maximum Likelihood 16

MHz Mega-Hertz 17

MTBF Mean Time Between Failure 44

PCB Printed Circuit Board 51

PSD Power Spectral Density 62

PV Process Variation 14

RF-DNA Radio Frequency Distinct Native Attributes 2

RGB Red-Green-Blue 70

RLC Resistance-Inductance-Capacitance 32

ROC Receiver Operating Characteristics 24

ROI Regions of Interest 66

SNR Signal to Noise Ratio 18

SPICE Simulation Program with Integrated Circuit Emphasis 29

SSD Solid State Drive 30

SVM Support Vector Machine 14

TDDB Time Dependent Dielectric Breakdown 3

TVR True Verification Rate 24

URE Unintentional Radiated Emissions 7

US United States 2

VLSI Very Large Scale Integration 44

INTEGRATED CIRCUIT WEAR-OUT PREDICTION
AND RECYCLING DETECTION USING
RADIO-FREQUENCY DISTINCT NATIVE ATTRIBUTE FEATURES

I. Introduction

1.1 The Problem

Globalization of the semiconductor industry has dramatically increased the probability of encountering questionable electronic components [51]. Because of the cost to maintain state-of-the-art electronics, control over all steps from design, manufacturing, validation testing and production distribution is very rarely maintained by a single entity [51]. As a result, multiple points of potential compromise exist in the electronics supply chain with products exchanging many hands between the design and final product fulfillment. Threats range from the contracted manufacturing foundry releasing parts that are sub-par or producing more copies than authorized, to groups recycling parts from old equipment and re-introducing these parts as new in the supply chain [27]. The predominate threat is recycled components, accounting for 80% of counterfeit incidents [25]. Using recycled components in place of new parts introduces reliability and early failure issues which can be catastrophic in applications requiring trustworthiness such as safety of flight in aircraft. The recycled component example may not be a security concern, as the parts do provide their intended function, but the next step of foundries or un-contracted firms inserting extra, Trojan, hardware and releasing those parts into the global supply chain is not unfathomable.

The global supply chain challenges raise concerns of reliability and security across the spectrum of end users with the government and military primary concerns of reliability and security to commercial industry concerns of economic cost and lost market share and protection of intellectual property. Previous Radio Frequency Distinct Native Attributes (RF-DNA) efforts at AFIT have focused on hardware security [65, 12, 11]. This work expands upon those efforts be examining the robustness of RF-DNA techniques by applying electronic wear-out to test articles and determining if RF-DNA can identify aged devices and ultimately identify recycled components.

1.2 Operational Motivation

Cyber-security of hardware devices is an increasing area of interest for the United States (US) Department of Defense (DoD). The majority of ICs are manufactured outside the US from potentially untrusted sources [45]. These untrusted sources have produced ICs of questionable quality resulting in electronic component failure [72]. Additionally, due to the prolific use of IC in today's modern electronic systems and the fact the US DoD had no comprehensive IC certification program as recently as 2006, the opportunity for malicious activities abound [16].

The proliferation of counterfeiting also raises concerns of maintaining the semiconductor industrial base. In 2011, the loss of revenue from copied and recycled parts was estimated by the Semiconductor Industry Association to run over $200 billion every year [45]. Maintaining electronic components sources from trusted manufacturers is a long term security concern potentially greater than isolated and targeted malicious activities.

Previous RF-DNA efforts have shown the potential to combat these concerns with malicious operation detection and hardware discrimination using the URE from an IC [12, 15, 14, 13, 15, 11, 54]. One RF-DNA application targets the ability to initially identify suspect parts before they are utilized in some application. Use of

RF-DNA to monitor changes in components, either from replacement with Trojan components or changes in operation from malicious software was explored by previous AFIT research [65]. This research effort seeks to determine the robustness of these previous RF-DNA cyber-security applications over the operational lifetime of an IC.

Over an IC's lifetime some characteristics of the IC's operation degrade. For example, Lau, et al. showed that a ring-oscillator's frequency exhibited a frequency reduction as the transistors in the ring-oscillator degraded due to Time Dependent Dielectric Breakdown (TDDB) wear-out [38]. TDDB is the degradation of a Field Effect Transistors (FETs) gate insulator insulating abilities that results in a reduction of a transistor's transconductance value [38]. A drop in transconductance reduces a transistor's current drive capability. The reduction in drive current reduces the switching speed of a digital circuit built from FETs. If the switching speed slows so far as to violate digital circuit timing requirements, an IC fails to function correctly.

Many of the common wear-out mechanisms such as electro-migration and Bias Temperature Instability (BTI) have the same impact as TDDB degrading current drive capability [44, 75, 29]. The physical changes as an IC degrades may not manifest as circuit failures or result in corrupted data for some time as manufacturers build design margins (process corners) to allow for these exact wear-out concerns [78, 75, 1]. The function of an IC can still be correct as long as the variations due to wear-out do not exceed the design margin.

RF-DNA utilizes the unique variations of an electrical system/component imparted to the device during its manufacturing process [12, 39]. The uniqueness of like designed components (parts design to be exact copies) may come from the manufacturing process variations that do not exceed the design margin. Unfortunately, these unique characteristics of an IC may not be static due to the physical wear-out changes previously mentioned. This lead to the fundamental question of this research: *Does* *physical IC wear-out impact RF-DNA?*

Operational Need - Improved Security and Reliability: Time varying attributes may be utilized for additional cyber-security applications, adding the ability to identify hardware tampering and recycled parts, to the already envisioned detection of Trojan hardware and software modification.

1.2.1 Security: Anti-tamper

The construct of training on known authentic devices and then comparing unknown devices to that training reference may be expanded to a series of timed reference signatures. If wear-out phenomenon has a repeatable impact, the application of RF-DNA to determine if a device is authentic vs. suspicious may be expanded to determine if an authentic device followed its assigned mission. For example, an autonomous system may be tasked to perform a mission for one year. If the golden reference is known at the year point, a physical layer security method can be implemented at the end of the year to verify the system has not been modified.

1.2.2 Reliability: Recycled Parts

URE RF-DNA was initially focused on identify intentionally altered hardware for example hardware Trojans and devices from untrusted foundries. However, if changes imparted from wear-out are observable using RF-DNA techniques, the ability to identify recycled components, even if they were at one point from a fully trusted source, may be achievable. Because URE RF-DNA techniques are non-destructive this capability might allow 100% parts screening before use in applications requiring high reliability.

1.2.3 Life-cycle Cost: Lifetime Estimation

The previous applications focused on security concerns by ensuring trusted and reliable electronic components. If wear-out modifications are traceable, RF-DNA may also provide a new tool to improve the life-cycle costs of electronic systems.

Operational Need - Lifetime Monitoring Lowering Life-cycle Costs: Using RF-DNA to monitor IC wear-out phenomenon may lower the life-cycle cost of electronic system maintenance by enabling closed-loop monitoring for preventative maintenance rather than early replacement based on statistical projections or replacement-after-failure schemes.

IC manufactures find themselves in an economic balancing act to provide the latest best performing ICs that have reliable lifetimes. Manufacturer's warranty claims related to early IC failures totaled eight billion dollars in 2011 [55]. Modern transistor fabrication calls into question the typical accelerated testing technique for estimating IC lifetime [50]. As a result, IC manufacturers list lifetime estimates that are lower than actual usable lifetime and they may also reduce a product's performance to ensure acceptable warranty claims [44].

Instead of relying on de-rated statistical lifetime estimates, RF-DNA may provide a means to track an IC's physical degradation during actual use. Monitoring an IC's degradation in a closed loop fashion could allow preventative/prescriptive maintenance on electronics rather than early replacement based on statistical projections or replacement after failure. Real time monitoring also allows throttled performance (balancing remaining lifetime for performance improvements). Throttling has been in place as a means to enhance performances for some time, but using the same monitoring techniques to extend lifetime is becoming more common. IC wear-out concerns have led IBM to incorporate on-chip ring-oscillator sensors in the z196 server that detect aging phenomenon [74]. Knowing the degradation allows the z196 server to actively manage performance and extend operation lifetime by throttling back on clock and timing settings.

All wear-out monitoring techniques researched during this work utilized circuits that are intended to be added to the IC die during manufacturing [38, 74, 82, 23, 30]. Most were variations on observing a reduction of a ring-oscillator's frequency as age phenomenon reduces transistor performance. The reliance on including additional test features (the ring oscillator) during fabrication prevents legacy (already built and or in use) systems from utilizing closed loop monitoring. However, RF-DNA does not require test structures built into the IC, but only the ability to place a near field probe in close proximity to an IC's packaging. If RF-DNA can track changes due to aging, the advantages afforded by close loop monitoring may be applied to legacy systems.

1.3 Technical Motivation

The technical motivation for this research stems from the question raised in Section 1.2; Does physical IC wear-out impact RF-DNA? Two additional questions that may be answered during this research include:

1. Do RF-DNA fingerprints have limited lifetimes; is sequential training needed to maintain accuracy?

2. Can the observation of device wear-out lead to an understanding of what mechanisms contribute to the device-to-device variations in RF-DNA?

Regarding Question 1, if RF-DNA fingerprints do lose accuracy as a function of a Device Under Tests (DUTs) operational time, the rate at which such degradation occurs may be allowable or dictate a retraining time-line to ensure a desired security level. This research indeed demonstrates accuracy degredations.

Regarding Question 2, anything that may alter the DUT's near field URE could potentially introduce the variations used to discriminate devices. In previous URE RF-DNA research all DUTs were assumed to be correctly manufactured with no malicious nor altered from specification hardware and all IC dies were packaged in identical form factors [15, 14, 13, 54, 65]. Given these testing scenarios the device-to-device variation was believed to result from IC die process variations created during manufacturing [12, 39]. However, the device-to-device variation may also be impacted by packaging variation (variation in the wire bonding leads to the package pins) which was proposed as a security measure by Gerald DeJean from Microsoft Research [18]. This research effort will bolster the belief that the RF-DNA variation is dominated by the IC die variations, since the aging/wear-out methods used focus on altering the semiconductors on the IC die and not the packing. The thermal process used for accelerated aging, described in Section 3.1.4, employed gradual temperature changes to minimize URE alterations from package modifications.

Technical Motivation: Determine the impact of IC wear-out on current URE RF-DNA Fingerprinting.

1.4 Goals

This work explores the impacts from Integrated Circuit (IC) wear-out on RF-DNA applications using Unintentional Radiated Emissions (URE) side channels. The three specific goals are to determine:

1. If transistor wear-out alters the accuracy of current URE RF-DNA device discrimination. Henceforth called *Device Discrimination.*

2. If RF-DNA can estimate device age, how long a device has been in operation. Henceforth called *Age Estimation.*

3. If RF-DNA can utilize wear-out changes in URE to identify aged (old/used) vs. un-aged (new/un-used) devices. Henceforth called *Age Discrimination*.

The third goal was not an initial desired outcome, but became an apparent opportunity based on the results of the first two goals. This last effort is a simplification of the second goal conducting a binary rather than a multi-age determination.

1.5 Research Contributions

Research contributions highlight limitations to existing RF-DNA capabilities as well as demonstrate new RF-DNA applications. These results are only directly applicable to the MSP430 micro-controllers used in this study, but the outcomes indicate potential problems, solutions, and applications for the RF-DNA process as applied to any device.

1.5.1 Existing RF-DNA Limitations

The operational construct of RF-DNA consists of initial training using items that are know to be correctly operating and trusted without any suspicion of compromise in security or reliability. This initial training results in a *golden reference* by which all future testing events are compared. The comparison to the *golden reference* is then used to determine if a device can by trusted. Passing the RF-DNA test might then allow a component to be used as a subcomponent in a system, grant access to a secure network, or result in trusted data from the system.

RF-DNA Fingerprint Longevity

This research demonstrates the *golden reference* may not be usable for all time; URE RF-DNA fingerprints have limited lifetime applicability. Maintaining a given level of device discrimination may require re-training at predetermined intervals. The initial *golden reference* loses accuracy when used with devices that have additional operational time. In this work, training references created after some initial burn-in time retain accuracy for a greater range of operational time than the initial reference.

Alignment Errors

Using URE RF-DNA requires collection of electro-magnetic signals that were never designed to radiate. To capture these emissions a narrow beam-width near-field probe is placed in close proximity to the test device. The fine beam-width is required to minimize noise and optimize the pick-up of the integrated circuits unintentional emissions. Unfortunately, this fine beam-width also introduces the need for consistent positioning over the test device. Slight misalignments may produce drastic changes in the captured unintentional emissions.

This research attempted to reduce misalignments by physically controlling device and probe placement using an alignment jig described in Figure 3.21 of Section 3.1.5. However, the impact of repositioning errors was still observable and produced a reduction in discrimination accuracy, as seen in Figure 4.38 of the Section 4.1.3. For *Device Discrimination*, the fine probe alignment protocol used in previous work, which focused on a single location with greatest URE power, may be required to align every location when spanning the entire device surface [65].

However, the multi-device training techniques used to undertake *Age Estimation* and *Age Discrimination* did reduced reposition errors as shown in Figure 4.40 of the Section 4.3.2. Multi-device training briefly mentioned below is fully explored in Section 3.1.6 and Sections 4.1.3 and 4.3.2.

1.5.2 New Techniques

Multi-location Fingerprints

The research work imparted wear-out changes to the test devices as described in Section 3.1.4 and 3.1.5. The specific impact of this wear-out on device URE, while hypothesized in Section 2.4, was not known prior to signal collections. As a result, URE signals were collected at multiple locations across the test device. Multiple locations increased the probability of finding a URE that captured wear-out artifacts. Initial efforts attempted to identify a few locations that displayed the greatest wear-out variations and use those locations to conduct the wear-out study. Unfortunately, consistent results could not be obtained across all test devices using the same locations. Fortunately using RF-DNA fingerprints which incorporated multiple locations provided repeatable results. Success of the multi-location fingerprints demonstrates the previous research technique to identify the best single device locations, as mentioned in Section 2.2.1 may not provide the best results.

Cross Device Training and Utilization

The *Age Discrimination* efforts trained reference classes using multiple devices and multi-location fingerprints. Such class definitions resulted in reduced reposition errors and allowed the application of RF-DNA techniques to devices not included in the original training set. This multi-device training reduced the ability of RF-DNA to train on device-to-device characteristics but instead forced training on attributes that are only due to wear-out alterations. Because of the multi-device training, the results for *Age Discrimination* demonstrate the ability to apply RF-DNA using a subset of devices to a larger population. For RF-DNA to find widespread application, the ability to apply a subset to a larger set is required.

1.5.3 New Applications

This research envisioned applying RF-DNA to provide a real-time continuous monitoring of device operation time. Using the techniques describe in this work, continuous monitoring (*Age Estimation*), was not achievable. However, the ability to determine if a device was new or used, *Age Discrimination* was achieved. This ability along with the applicability to devices not in the training set implies RF-DNA may be usable to screen recycled components.

1.6 Document Organization

This document is organized in the following remaining chapters. Chapter II first provides a summary of existing methods and how RF-DNA using URE may provide another tool to defeat counterfeiting. Chapter III presents the methodology used to explore the three research goals. Chapter IV documents the performance achieved using the methods of Chapter III. Chapter V provides a summary of results and proposed means to improve the performance and expand the capabilities presented in this work.

II. Background

This chapter provides greater detail on the ideas mentioned in the Introduction. Existing methods to defeat counterfeiting are briefly mentioned. Next, the RF-DNA process utilizing URE variations is described. After the RF-DNA process, potential causes of URE variation are enumerated. Wear-out impacts to URE are then explored. In both of these two URE sections, manufacturing methods used to mitigate variation are also mentioned. The final section discusses the impact of wear-out on the RF-DNA process. The seminal works applying RF-DNA to URE side channels were accomplished by William Cobb and Samuel Stone at the Air Force Institute of Technology (AFIT) [14, 15, 12, 11, 54, 64, 65]. Their works will be used as primary examples to frame this wear-out study.

2.1 Current Techniques Addressing Counterfiets

The methods to defend against utilization of counterfeit electronic devices fit into two categories. The first category, provides a *chain-of-custody* accountability on all parts in the supply chain. The second category implements some form of *hardware validation* before acceptance of a device. This research effort falls into the *hardware validation* category and proposes the use of RF-DNA as a tool to provide the validation.

Chain-of-custody is implemented by either placing a unique identifier or providing administrative checks at multiple points throughout the entire supply chain from design through production and distribution up to final consumer acceptance [59]. For example, according a Government Accountability Office report, the Defense Logistic Agency validates contract parts with a botanically-derived marking on all high-risk microcircuits [71, 25]. These procedures ultimately rely on trusted agents to conduct the validation steps and correctly impart a unique label on each component. Because these techniques rely on trusted agents they are still susceptible to counterfeit intrusion should the agents be compromised or incorrectly apply identifier markings.

Hardware validation reduces the requirement of multiple trusted agents and provides for counterfeiting solution at a single point of control. The single control point may unlock *hardware encoded* security, conduct *physical inspections*, or screen devices for some *intrinsic features* determined to only exist on non-counterfeit parts. RF-DNA utilizes intrinsic features when it trains and utilizes the distinct native attributes of devices.

Hardware encoded security, requires the manufacturing foundry place dedicated components on the target integrated circuit where only the rightful intellectual property owner can unlock the device [25, 51, 31]. By tracking the number of devices from the foundry with paired unlocking keys, only non-counterfeit devices can be unlocked thus preventing counterfeit devices from functioning. However, this technique still uses a trusted agent (the foundry) to correctly impart the encryption and is only available for new products. Additionally, this technique does not identify authentic but recycled devices within the supply chain. Identifying recycled parts would required administrative tracking of a device's intial use.

Physical inspection does not require special encryption components and can be used for both newly manufactured as well as legacy parts. This technique analyzes characteristics that are different between authentic and counterfeit parts. These altered characteristics can come from inspecting packaging alteration, various imaging techniques, and electrical performance parameters [25]. Unfortunately, most of these physical inspection techniques require high cost equipment or specially trained subject matter experts and considerable time to determine counterfeit status. Examples of these actions range from inspecting IC package alterations like surface damage and relabeling of part numbers or altered package pins from desoldering to using x-ray imaging to determine interior IC die changes indicating differences from authentic devices. This method has the ability to identify counterfeits that are altered from original design parameters as well as discover originally authentic devices that have been recycled.

Intrinsic feature screening uses some inherent signature or collection signatures that differ between authentic and counterfeit devices. These features are intrinsic to the devices meaning no additional hardware is required during manufacturing [25, 27]. Ideally these features are also un-copyable. Utilization of IC variations imparted from manufacturing Process Variation (PV), further explained in Section 2.3.2, is a prime method to accomplish this screening.

Intrinsic feature screening differs from *physical inspection* methods in that *intrinsic screening* does not look for specific indicators of altered components but instead trains a system to identify what is normal for an authentic device. With this training established, the screening process rejects devices that do not fit the norm. After initial training, the system may conduct screening without the need for subject matter experts needed to interpret the results or run specialized equipment as in the case with *physical inspections.*

Machine Learning techniques are applicable to finding the *intrinsic features* that support counterfeit and recycled parts screening. An example of this technique utilized Support Vector Machine (SVM) to separate new vs. recycled Digital Signal Processing (DSP) circuits using 49 early failure parametric test measurements [27]. The parametric test data was generated from proprietary manufacture testing that prevents release of parts that would fail too early in their operational life. This data was used as it requires no additional signal collection above what manufactures already accomplish. This effort was able to identify new vs. used devices with varying age between 95 - 100% accuracy when determining the category of a group of devices, but with only 69 - 92% accuracy when determine the status of a single device.

RF-DNA is an application of machine learning that has it roots in determining counterfeit vs. authentic devices as it applies to altered or Trojan hardware modification. RF-DNA using URE differs from the support vector machine example above as it does not require proprietary test data and RF-DNA can be applied to specific hardware applications using *in-situ* collections vs. isolated testing data. The remainder of this work examines the impact of IC wear-out on the existing construct of counterfeit hardware modification detection, *Device Discrimination*, and is the first effort to expand RF-DNA to recycled part detection, *Age Estimation* and *Age Discrimination.* As a comparison to the SVM example, this work achieved an average new vs. recycled correct detection rate for individual devices between 78.7 - 99.9%.

2.2 RF-DNA Process with URE

Previous RF-DNA efforts used unique variation between test devices in order to discriminate multiple devices from each other. The term Machine Learning is used instead of RF-DNA in the last steps as RF-DNA is a specific utilization of machine learning with inputs defined by the RF-DNA process. The general process to conduct RF-DNA discrimination consists of five steps:

1. Signal Collection

2. Signal Filtering

3. Fingerprint Generation

4. Machine Learning Training & Use

5. Machine Learning Results & Performance

The first three steps culminate in vectors (array of numbers) that capture the uniqueness of the various Devices Under Test (DUT). These vectors, called *fingerprints*, can be generated using any technique that captures desired variations. For example, previous RF-DNA work has utilized different signals such as time domain voltage recordings from an oscilloscope, correlation coefficients from matched filtering, and some custom built demodulation measurements [63, 8, 7].

All steps to generate fingerprints are repeated for multiple signal bursts for each DUT. The multitude of fingerprints provide the machine learning with enough signals to determine characteristic distributions for each trained class. The machine learning can then determine a model that defines characteristics for each trained class. With each class defined, the fingerprints from unknown devices are compared to the trained model and the best fit is selected for the unknown device.

No matter the type of initial signal used for Fingerprints generation, the last steps use machine learning to generate means to classify or verify the DUT identity. Multiple machine learning techniques exist but RF-DNA typically relies on Multiple Discriminate Analysis / Maximum Likelihood (MDA/ML) or Generalized Relevance Learning Vector Quantization Improved (GRLVQI) [15, 65, 2, 42]. Examples in this explanation will strictly use time domain voltage signals from an oscilloscope.

2.2.1 Step #1: Signal Collection

RF-DNA using URE collects signals using a near-field Electromagnetic (EM) probe and an oscilloscope system like the Riscure side channel platform [52]. Signal collections are accomplished at a sampling rate much higher than the Nyquist criteria for the DUT's clock frequency [46]. In Cobb's work, the oscilloscope sample rate was 2.5 Giga-Samples per second (GSps) and a Low Pass Filter (LPF) of 1-Giga-Hertz (GHz) was used between the EM probe and the oscilloscope even though the

DUTs had a clock frequency of 29.48 Mega-Hertz (MHz) [65]. Capturing the signals in such a way allows the ability to empirically determine the best signal processing technique to capture the desired DUT variations.

In addition to correct sampling rate, the EM collections require consistent physical alignment with the DUT. The EM probes used by both Cobb and Stone provide a fine beam-width that is nominally smaller than the DUT's physical dimensions. As a result, multiple probe locations may be used to conduct RF-DNA discrimination. To minimize unwanted URE variations due to probe placement shifts between devices both Cobb's and Stone's effort used a single location for all signal collections. The single location corresponded to the maximum power emitted at the DUT's operating clock frequency [65, 15]. Cobb used a jig to hold the DUTs in a fixed position. Whereas Stone used a coarse alignment marker on the DUT followed by an alignment program to correctly place the EM probe for all collections [15, 65].

This wear-out study collected signals at multiple locations for each DUT. Multiple locations were used because it was unknown which location will be most impacted by wear-out changes. The alignment jig was the only physical alignment technique employed. The additional time required for Stone's correlation alignment technique was time prohibitive when collecting signals for multiple locations across multiple devices. This wear-out study only provided limited time to collect emissions between each successive age.

Finally, timing alignment is required between all DUT URE collection bursts because changes in operations from the DUT will also alter the URE [65]. If the specific application of RF-DNA seeks to detect changes not stemming from altered operations, collections require operations/timing alignment. Cobb's collections utilized a trigger signal to synchronize oscilloscope recordings [15]. Stone's efforts used a correlation program to align recordings after collections eliminating the need for a physical trigger signal [65]. This wear-out effort employed a trigger signal again to minimize collection time between successive wear-out ages.

2.2.2 Step #2: Signal Filtering

While the signal collection step is concerned about minimizing controllable variations from physical or timing misalignment, the filtering step is concerned with providing the best Signal to Noise Ratio (SNR) from the collected signal before Fingerprints are calculated in Step #3. In URE RF-DNA the signal component of SNR is any parameter that provides greater discrimination. Noise is likewise any parameter that when minimized improves discrimination. For example, noise may include traditional concepts such as Additive White Gaussian Noise (AWGN). But noise may also encompass unneeded segments of the collected signal.

The filtering step is improved by knowledge of the expected signal variations. In this wear-out work, the signal collections around clock transitions proved to be the location of signal and the collections between clock transitions effectively functioned as noise. This SNR as a function of location around the clock transitions is further explained in Section 3.1.7 of Chapter III - Methodology. Another examples of custom filtering is seen in Carbino's work where RF-DNA was calculated for intercepted data packets using the near-field side channel of an Ethernet cable [7]. Custom matched filtering was used to decode the Ethernet side-channels before fingerprint generation was accomplished. In other works, collected signals were down-converted to an intermediate frequency or transformed to frequency domain data using Fourier transform or wavelet transforms [32, 76]. The filtered and transformed signals may be more useful than using the raw oscilloscope time domain collection. Application of knowledge regarding what signal characteristics may capture the underlying desired discrimination occurs in the filtering step.

Some RF-DNA efforts intentionally add AWGN to the collected signal. The noise is added to test the classifiers ability to correctly identify devices in simulated degraded/noisy conditions. This effort performed all exercises at the collect signal's SNR and no AWGN was added. Instead of AWGN, the induced wear-out for each device was the effective noise which tested RF-DNA's capabilities.

2.2.3 Step #3: Fingerprint Generation

RF-DNA fingerprints for a time-domain signal are generated by calculating the 2nd, 3rd and 4th central moments (σ^2-variance, γ-skewness, and $\varkappa$-kurtosis) as applied to the instantaneous amplitude, phase, and frequency of the collected signal [65, 15]. The standard deviation (σ) is also included as a fourth statistical feature. Equation (2.1) describes how to calculate μ_X, the mean, used in the central moment calculations that follow. Expressions (2.2) - (2.4) provide the formulas for calculating the central moments. Equation (2.5) defines the standard deviation as the positive square root of the variance. The signals used to form RF-DNA fingerprints are collected as discrete, digitally sampled oscilloscope traces and therefore all the formulas used are the discrete forms and not the continuous forms. For the remainder of this paper, the collection of these four statistics will be referred to as the *moments*, even though the standard deviation is technically not a central moment.

$$\mu_X = \frac{1}{N_X}\sum_{n=1}^{X_N} x(n) \tag{2.1}$$

$$\sigma^2 = \frac{1}{N_X}\sum_{n=1}^{N_X} \left(x(n) - \mu_X\right)^2 \tag{2.2}$$

$$\gamma = \frac{1}{N_X\sigma^3}\sum_{n=1}^{N_X} \left(x(n) - \mu_X\right)^3 \tag{2.3}$$

$$\kappa = \frac{1}{N_X \sigma^4} \sum_{n=1}^{N_X} \left(x(n) - \mu_X\right)^4 \tag{2.4}$$

$$\sigma = +\sqrt{\sigma^2} \tag{2.5}$$

The moments are calculated for all three *signal attributes*: instantaneous amplitude-$a(n)$, phase-$\phi(n)$, and frequency-$f(n)$. The $x(n)$ values in Equations (2.1) - (2.4) are set by each signal attribute as defined in Equations (2.6) - (2.8). The in-phase (I_{TD}) and quadrature-phase (Q_{TD}) components of the time domain signal (S_{TD}) are defined by Equation (2.9). The in-phase values (I_{TD}) are the real valued oscilloscope collected signals. The quadrature-phase values (Q_{TD}) are calculated using the discrete Hilbert transform.

$$a(n) = \sqrt{I_{TD}^2(n) + Q_{TD}^2(n)} \tag{2.6}$$

$$\phi(n) = \tan^{-1}\left[\frac{Q_{TD}(n)}{I_{TD}(n)}\right] \tag{2.7}$$

$$f(n) = \frac{1}{2\pi}\left[\frac{\phi(n) - \phi(n-1)}{\Delta n}\right] \tag{2.8}$$

$$s_{TD}(n) = I_{TD}(n) + jQ_{TD}(n)\ . \tag{2.9}$$

These fingerprints are intended to capture the uniqueness of each device as each device has slightly different URE. Because the moments are a type of average, very minute changes across a device may be masked when calculating the moments for the entire collected signal. The uniqueness between identically designed ICs running the exact same operations may only occur in very small time slivers within an entire signal.

As a result, the signal is divided into multiple subregions. With more subregions, the uniqueness of each devices can have a greater impact when calculating the four moments for each subregion. However, the number of subregions can not grow without bound. Too many features may prevent a classifier from creating a usable model, computation time becomes too long and storage requirements grow too large.

The optimal number of subregions for a given signal or sequence is a trade off between accuracy versus speed of the classifier. In Cobb and Stone's work the number of subregions was determined empirically. Cobb's efforts generated subregions based on the PIC's clock frequency. Cobb's signal collections encompassed 32 clock transitions and he determined 32 ($1 \times f_{clk}$) subregions performed better than 64 ($2 \times f_{clk}$) or 16 ($\frac{1}{2} \times f_{clk}$) subregions [15]. Stone settled on $N_{SR} = 12$ subregions for his 10 operation sequence [65]. The choice of N_{SR} used in this work is explained in Section 3.1.7.

With these subregions defined, a single fingerprint becomes the array of moments over all signal attributes (amplitude, phase, frequency) for each of the subregions. The four moments may also be calculated for the entire signal. If the total signal is used, the moments are appended at the end of the subregion elements for each signal attribute. Figure 2.1 provides a graphical representation of fingerprint generation/construction, without utilizing the total signal moments. The four moments are calculated within each subregion (SR) for each signal attribute (SA). The array of statistic numbers along the top row of the figure shows the organization of all the moments. The collection of top row variables is a single fingerprint vector for a single collection burst.

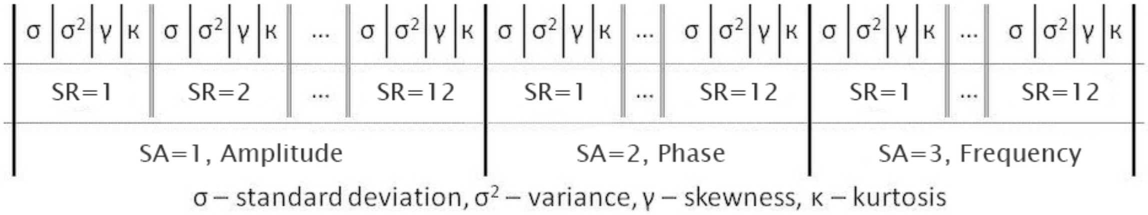


Figure 2.1. Fingerprint Construction. The array of all statistics numbers is a single fingerprint.

2.2.4 Step #4: Machine Learning Training & Use

MDA/ML

MDA/ML performs classification by projecting input data (the fingerprints generated in step #3) from higher dimensional space (the total number of features/moments in a fingerprint) down to a hyperplane with dimension equal to one less then the number of classes, $N_{cls} - 1$. The projection is a linear transformation that maximizes the distance between classes while simultaneously minimizing the intra-class scatter on the hyperplane [12, 2]. Training of the MDA/ML classifier determines the projection matrix that performs the optimal linear transformation. This training is done with a sub-set of collected fingerprints. The training methods used for this research are explained further in Chapter III.

Device discrimination then applies the projection matrix, developed during training, to the fingerprints for each device that requires discrimination. As a result the multi-dimensional fingerprints related to each DUT are projected down to the $N_{cls} - 1$ hyperplane. Selection of a class is completed by choosing the class with the maximum likelihood, or best fit, to the each of the test device's projections on the hyperplane [12]. The best fit determination can use simple Euclidean distance, or other scores such as Mahalanobis distance [2]. The percent correct average used to measure performance is the percentage of all testing fingerprints that are classified correctly. This discrimination process of determining device type is historically labeled as *Test-*

ing in previous RF-DNA work. In this work the terms *projection, use, and testing* all indicate device determination using the projection matrix as just described.

Figure 2.2 shows an MDA/ML example of a four-class scenario. In this case the 3-dimensional hyperplane provides an intuitive / visualize-able problem. Each cluster of the four different colors is a distinct class. Each individual circle is one instance of a device. The spread of all the individual circles around each class mean is the intra-class scatter. This 3-dimensional hyperplane best separates the four clusters while at the same time keeping the intra-class scatter within each signal cluster minimized. The block dot signifies an instance of an unknown device type projected down to the 3-dimensional hyperplane. The black dot's class determination is then chosen as the light blue (top-right) class since the dot is closest in distance to the light blue class.

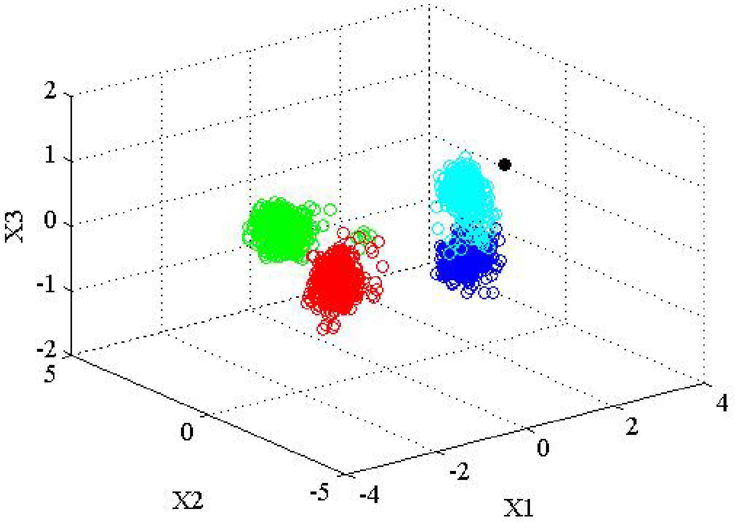


Figure 2.2. Four Class MDA/ML Projection to 3-Dimensional Hyperplane

GRLVQI

GRLVQI was used for some initial data analysis and is therefore briefly introduced here. GRLVQI was not used for its classifier function due to its longer run time. MDA/ML completed one classification run on average in about 30 seconds. GRLVQI required around one hour for a single classification run. This study ultimately required hundreds of classification runs. Therefore, GRLVQI was time prohibitive for the final wear-out studies. GRLVQI was used for some data dimension reduction and only applied to the age estimation effort of the three goals.

GRLVQI was developed for high dimension classification problems where the many input dimension may have complex interaction and intuitive understanding of each dimension's importance to classification is not known [42]. Unlike MDA/ML where every input feature's value has an impact, although some may be extremely small based on eigenvector dimensional weights, GRLVQI only uses features that are determined to provide information useful in the classification process. GRLVQI's wrapper technique ignores input features that have minimal impact to class separation [42, 33]. GRLVQI separates the classes by placing prototype vectors around the periphery of each class in between the space adjacent to all the classes. The training of GRLVQI is the process of placing the prototype vectors in the correct locations to maximize the margin of correctly classifying each of the training events based on the training data set [34]. Class selection in GRLVQI is then completed by selecting the class of the prototype vector that is closest to the input vector of the tested device.

2.2.5 Step #5: Machine Learning Results & Performance

Performance results are historically presented with two metrics. The first metric plots the average correct classification as a function of SNR. The second method uses Receiver Operating Characteristics (ROC) curves to display how well the discrimination separates devices with both correct determinations, True Verification Rate (TVR), and false positives, False Verification Rate (FVR).

A representative classification performance vs. SNR plot is shown in Figure 2.3. The plot indicates how well a trained classifier correctly labels a DUT. In the 10dB

SNR scenario (AWGN added to the collected signal to produce a 10 dB SNR) all instances of Dev-1, 6 and 7 were identified as Dev-1, 6 or 7 with just under 100% accuracy. However, all the instances of Dev-2 & Dev-5 were only correctly labeled as Dev-2 or Dev-5 with 70% accuracy.

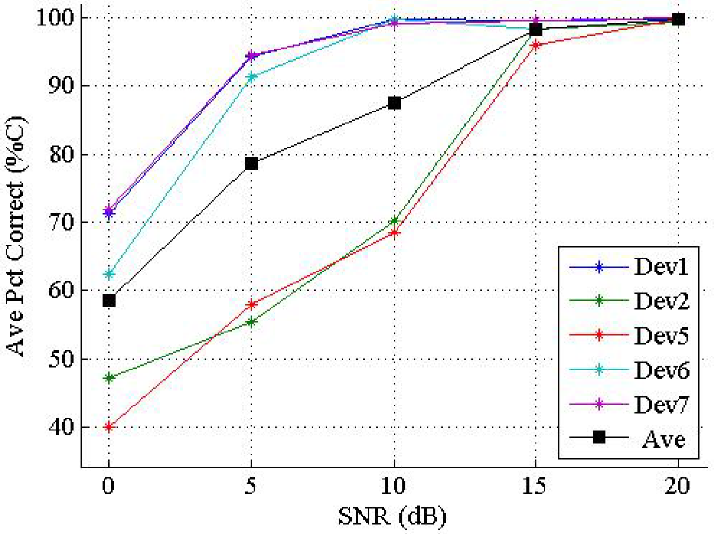


Figure 2.3. Classifier Accuracy as function of SNR. Traces document device identification accuracy for five classes.

The results of Figure 2.3 indicate how many times the classifier correctly selected a DUT's true class, but it does not explicitly indicate how many times a class was miss-identified as another class. For example, all the 10 dB SNR fingerprints for Dev-2 were called Dev-2, 55% of the time. However, this plot provides no information on how many times Dev-1, 5, 6, 7 were falsely labeled as Dev-2 to achieve the 55% classification performance. Classification performance for Dev-2 could be at 100% by calling all devices as Dev-2 for every test. Because of this possibly, the ROC curve is needed in addition to classification performance of Figure 2.3.

A single ROC curve displays the ability of the classifier to accurately accept or reject an event's claimed class. Each ROC curve trace is a binary test showing the results for a single device vs. the results for all other devices lumped into a single set.

Multiple ROC curves may be presented on one graph. Figure 2.4 shows the classifier's performance for the 5 dB results shown in Figure 2.3. From Figure 2.3, Dev-6 was correctly identified slightly above 90% of the time. From this ROC plot we see that in order to achieve 90% accuracy, devices that were not Dev-6 were incorrectly labeled as Dev-6 at a rate of roughly 6%. Dev-2 is less discriminable from the other classes. In this case, the Equal Error Rate (EER) is around 23% meaning that in order for this classifier to correctly identify all Dev-2 events 80% of the time, the model allows a miss-labeling of non-Dev-2 as Dev-2 at a rate of 23%. The EER is the point where the $FVR = 1 - TVR$ for each ROC curve. The traces for Cls-2 and Cls-5 in Figure 2.4 are dashed because they are below an $EER = 10\%$, while Cls-1, Cls-6 and Cls-7 are separated at or better an $EER = 10\%$.

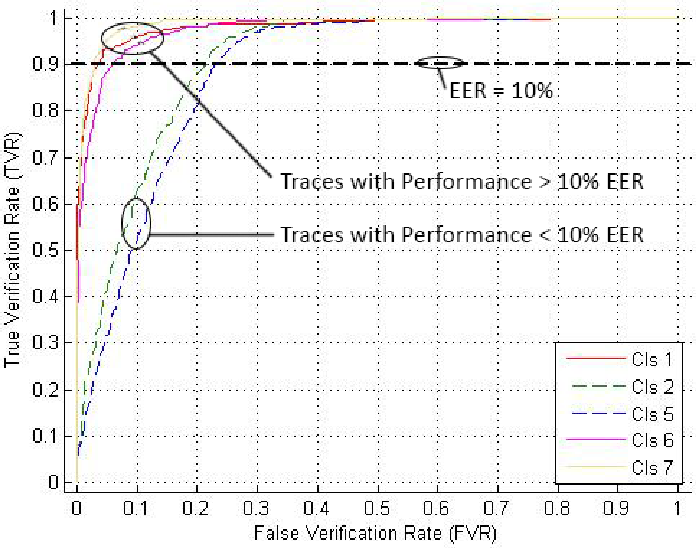


Figure 2.4. Class vs. Non-Class ROC at 5 dB SNR. Solid Lines indicate performance greater than 10% EER. Dashed lines show performance below 10% EER.

While the ROC curve is a tool used to display each model's class separability, each model (result of every machine learning training event) has its own ROC curve. In this wear-out work, consistency of results is a primary focus and there are between 36 up to 5000 machine learning training events. Therefore, results will not be presented with actual ROC curves. Instead, a histogram of false identification rates for all 36 to 5000 training events will be used. Using the histogram allows a single plot to display the collective results rather than using a large number of ROC curves. Providing results in a collective summary loses the ability to show the probability distributions and power for each individual training model. However, the histogram results provide an indication of the entire techniques ability to consistently provide device separation. Section 3.3.2 provides the details of this method.

2.3 URE: Fixed Hardware Variations

This section provides background to understand the causes of URE variations which are vital for RF-DNA device separation. Events that alter a device's operating current lead to changes in URE [47, 58, 67]. Device operation current is controlled and influenced by both software, the program running on the device, and the specific hardware in use for a given operations [65, 64]. As this work is focused on wear-out impact, the current alteration from software is not study by holding operations constant across all collections. Instead the influence of hardware on device URE is the sole focus.

2.3.1 Intentional Changes

Hardware changes may be intentional or unintentional. Intentional changes come from manufactures altering a device by design. Device improvements include actions like adding additional memory, for example, increasing a microprocessors cache size. Altered devices may provide additional functional components, such as floating point modules in different device options. In fact, the MSP430 micro-controller used in this study is available in 525 different configurations [69]. These different configurations offer low power versus high performance options, different display modules, input-output options, all in the same IC package. The case of Trojan hardware, while malicious rather than benevolent, is another example of intentional hardware changes.

The previous examples impart design/functional changes on the IC die. Other hardware alterations may maintain the same function but still impart hardware changes. Different process technology, how the manufacture builds an IC, can produce devices that provide the same function but are completely different on the inside of the package. Different fabs, one using Complementary Metal Oxide Semiconductor (CMOS) and another using SiGe BiCMOS, Silicon Germanium bipolar junction transistor CMOS, for the same mixed signal IC provides one example [49].

The pinnacle of hardware changes would be using an Application Specific Integrated Circuit (ASIC) versus a Field Programmable Gate Array (FPGA) for the same task. FPGAs and ASIC use completely different architectures. A micro-controller is a specific type of ASIC. ASICs typically complete tasks with the exact logic gates required for specific functions and are built with performance and speed in mind. Whereas FPGAs use generic logic modules re-configured for a function and reconfigurability is emphasized resulting in less performance and speed compared to an ASIC.

All previous RF-DNA URE efforts kept the DUTs within the same family (different revisions with extra memory of minor improvements). This wear-out study will use identically design and produced MSP430 micro-controllers. This experimental deigns includes no intentional changes. The only desired URE changes are due to the phenomenon described in the the next two sections.

2.3.2 Unintentional Changes: Process Variation (PV)

Manufacturers do their best to construct ICs without any of the following hardware variations. However, these changes are present at some level despite the efforts to minimize. The work of DiBene and Knighten using Simulation Program with Integrated Circuit Emphasis (SPICE) simulations showed the greatest change in URE emissions at multiple clock harmonics was attributable to process variation and not changes in the operating temperature nor applied voltage [19]. These minute hardware variations, called Pocess Variation (PV), while less affecting than intentional alterations, can not be ignored as explained in the discussion of Combating Variation in Section 2.3.3.

ICs are built in very controlled environments, but the multitude of fabrication steps creates many opportunities for PV. The potential exist for the multitude of slight variations to compound upon each other leaving an observable distribution of varying IC behavior. Variation during the steps required to build ICs such as lithography mask misalignment and varying temperatures during thermal processes allow opportunities for PV which result in IC transistors with slightly different dimensions and electrical properties [78]. These PV effects occur within a single IC die and across multiple IC die wafers [40]. As a result, no identically designed ICs are exactly the same. It is these PV artifacts which allow RF-DNA using URE to discriminate between identically designed devices.

2.3.3 Combating Variation

Timing critical paths are the typical limiting factor in IC performance speed [3]. In these parts of an IC, digital logic gates are cascaded. Correct values on the final output stage requires all the preceding logic gates to settle on intermediate correct logic values. Because of the cascaded nature the slight delay in each logic gate compounds. The adder is one example of a microprocessor functional component that requires extreme critical path design attention [35]. The functional unit is used in myriad mathematical operations and logic comparisons. Because of the propagation time required for correct logic values, this functional unit receives a lot of design attention to ensure correct operations at the maximum clock speed possible.

Design Margin or Guard Bands

The means to ensure correct operation is called the *design margin* or *guard bands*. Design margins either build robustness into a design, at the cost of additional IC die area, or de-rate, slow down the clock from max speed, to ensure correct operation for all envisioned process variation [35, 37]. The loss of performance can sometimes be up to 30% of the maximum possible if all PV was eliminated [75]. An observable example of this performance loss can be seen in over-clocking microprocessors in consumer personal computers where the consumer attempts to regain some of the de-rated performance.

Adaptive & Redundant Circuits

While still applying design margins, the inclusion of extra circuitry and monitoring circuits allow ICs to actively account for PV, ensure correct IC function and regain some of the de-rated performance. This exact practice is common for Solid State Drive (SSD) hard drives [66, 28, 68]. SSDs use flash memory that may have malfunctioning word line segments. A monitoring circuit that performs a continuity check can switch in extra FLASH memory banks to obtain the designed memory size.

Regaining speed performance from de-rated clock speed can use monitoring circuitry, called a canary circuit. The canary circuit provides feedback allowing a circuit to approach max speed for each specific circuit. This feedback learns the max speed for each instance of use and the de-rating is custom tuned for each PV case [75].

Use of adaptive or redundant circuits can be considered as a design parallel to Trojan hardware. Previous RF-DNA efforts have explored the cyber-security implications of Trojan hardware. This wear-out study does not intentionally exercise any adaptive or redundant techniques on the MSP430 micro-controller.

Binning

In some instances PV pushes actual operation beyond the manufactures design margins and the IC will not function at the intended specifications. However, such devices may still function at lower performance specs. This process of specifying an IC at lower performance values, called binning, allows a manufacturer to sell products at less than top-of-the-line market value [81, 56]. Binning is mentioned here to highlight the commonality of PV in semiconductor manufacturing. All MSP430 micro-controllers used in this study were manufactured to the same performance specifications.

2.4 URE: IC Wear-out - Variations over time

This section describes additional complexities that alter IC UREs. First, examples from systems concerned with Electromagnetic Compatibility (EMC) or Electromagnetic Interference (EMI), where changes in URE can violate electronic component compatibility, are used to demonstrate URE changes over device lifetime. Second, the fundamental physical changes that alter URE are described at the individual transistor level. Next, SPICE simulations are used to display observable wear-out current changes. Finally, the manufacturer methods used to mitigate wear-out are briefly discussed.

2.4.1 Electro-Magnetic Compatibility / Interference (EMC/EMI)

Circuit designers concerned with EMC attempt to limit problems that result from unintentional conducted (physical wire connection) and radiated signals altering the correct function of other circuits [6, 58]. RF-DNA turns the problems of URE into the means to discriminate different ICs. The remainder of this section uses EMC issues to highlight how aged ICs can alter URE and potentially RF-DNA applications.

During research readings a few simulation programs that estimate the EMI from chips were repeatedly mentioned [61, 10, 60]. These simulators attempt to reduce the complexity of a full-wave solver into a less complex model that can quickly (faster than a full-wave solver) produce reasonable results. The common practice among these efforts focused on characterizing the current flowing through Resistance-Inductance-Capacitance (RLC) wire runs. The current flow is modeled as current sources on the IC die driving the response of the internal wire runs represented with equivalent RLC loads as shown in Figure 2.5, reprinted with permission of IEEE. Z_{PCB} models the RLC impedance of the PCB. L_{MP} accounts for the inductance of the measuring magnetic probe and I_{MP} is the current induced in the magnetic probe measuring the circuit response. Z_{PKG} models the impedance of the device packaging. The LSI box is the IC package. Z_{LSI} captures the RLC impacts of the IC-die. I_i is the modeled current source representing the IC-die functions. The models focused on the current flowing through the circuit's power supply wire runs or areas of rapid current fluctuations in response to the IC die transistor operation. Consistent with the physics of Faraday's law and electro-magnetics, larger/faster current changes create stronger emissions.

The EMI references highlight two main take aways: current fluctuations are the driving factor in EMI near-field emissions, and the most dominate current fluctuations occur in power supply runs and areas of rapid current swings caused by switching of logic circuits. Given these two main points, any factor that modifies the current of an IC may alter the IC's near-field emissions. The collection of IC die transistors control the current flow. Changes to transistor switching characteristics will impact current

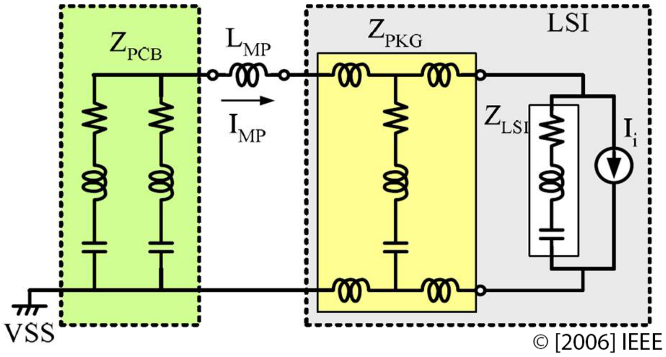


Figure 2.5. Linear Equivalent Circuit and Current Source Model, used to measure Electro-Magnetic Interference (EMI) emissions. [**67, Fig. 10**]

swings.

In addition to the process variation created during an IC's manufacturing, the switching characteristics of an IC can change over time as the device undergoes wear-out. These wear-out issues have become more of a problem as IC minimum transistor sizes have shrunk to nano-meter size dimensions [74]. The stresses imparted to these shrunk transistors even under nominal conditions (applied voltage, operating temperature) can be thought of as a type of age induced process variation. This age induced process variation also impacts an IC's EMI emissions as demonstrated in Figure 2.6 [6], reprinted with permission of IEEE. In this figure, a set of un-aged devices are characterized by their EMC emissions. The devices are then aged to induce wear-out phenomenon, with accelerated lifetime techniques that increase the rate of wear-out from years down to hours [17, 6]. After the aging, the EMC emissions are recorded and compared to the un-aged emissions.

Figure 2.7, reprinted with permission of IEEE, displays one example of measured change from the work of Boyer, et al in reference [6]. Three un-aged data sample produced a mean with a higher amplitude peak at a slightly higher frequency. The aged results produce means that are at reduced amplitude and lower frequency.

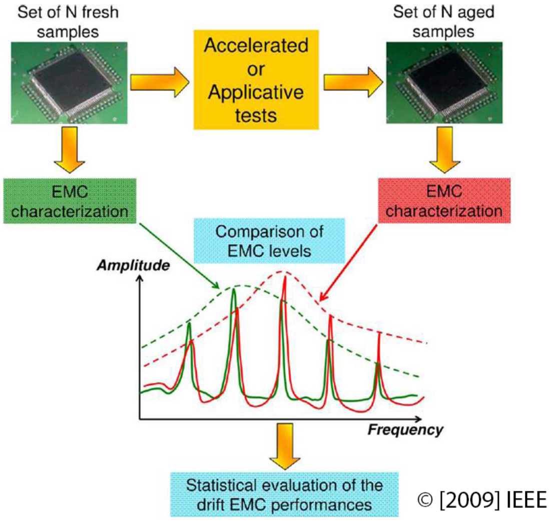


Figure 2.6. Age induced changes to Electro-Magnetic Compatibility (EMC) emissions. [6, Fig. 6]

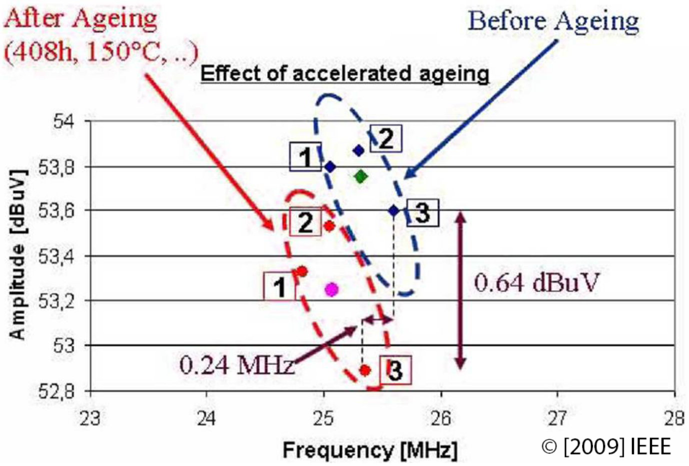


Figure 2.7. Age induced Electro-Magnetic Compatibility (EMC) emissions shift of the 26-Mhz harmonic. [6, Fig. 13]

2.4.2 Transistor Aging / IC Current Alteration

Section 2.4.1 described how URE is a function of IC current and how aging alters URE. Recall from the EMC discussion, the IC current is the driving factor for URE. This section explains how IC current changes due to transistor aging.

Each FET's current can be simply modeled by the equations shown in Figure 2.8 [75]. An IC die may have hundreds to millions of individual PMOS and NMOS transistors. The left images are the schematic symbols for a single PMOS and NMOS. The equations describe a transistor's current given the applied terminal voltages; the transistor can be in one of three states described by the conditions on the right. This model, called the long-channel model, is not accurate for modern FETs [75]. However, the long-channel model can be used to develop intuition about modern transistor performance variation as parameters of a transistor are altered by design, process variation, and wear-out/aging.

A FET is a four terminal device; with the body usually tied to the source terminal. The subscripts on the current equations signify the current direction through the terminals and polarity of the applied voltage on the terminals. The k_p and k_n values are constants that account for the mobility of the FET's channel carriers/current and width and length sizing of each transistor. Process variation that produces mask alignment variation or different dopant profiles would result in slightly different k_p and k_n values. The V_{Tp} and V_{Tn} are called the threshold voltages and these values control when the FET is considered to be on or off as channel current is functionally zero as compared to the on current. Process variation related to the thickness of an FET's gate insulators and doping profiles would cause slight variations in threshold voltage values. Such process variation fixed at IC manufacturing time have the potential to be the primary variations RF-DNA utilizes to discriminate devices.

The model used by the upcoming SPICE simulation, called BSIM3v3, accounts for many additional factors ignored by the long-channel model thus producing greater accuracy [43]. Unfortunately, this more complex model is not easily intuitive like the long channel model. Fortunately, the trends the long channel model predict are generally valid even with the more complex model; the quantitative values of the long channel model my be in error but the qualitative changes are still applicable. Therefore, the long channel model can be used to describe the qualitative changes

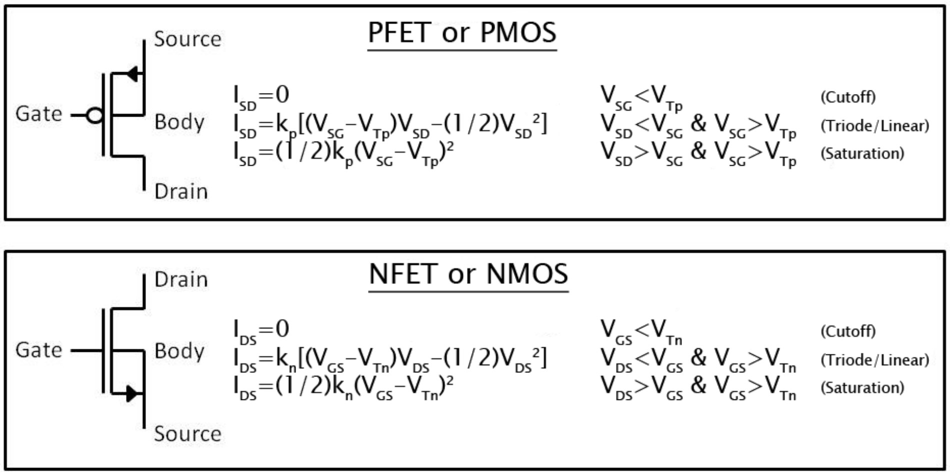

PFET or PMOS
Source
Gate
Body
Drain
$I_{SD}=0$ $V_{SG}<V_{Tp}$ (Cutoff)
$I_{SD}=k_p[(V_{SG}-V_{Tp})V_{SD}-(1/2)V_{SD}^2]$ $V_{SD}<V_{SG}$ & $V_{SG}>V_{Tp}$ (Triode/Linear)
$I_{SD}=(1/2)k_p(V_{SG}-V_{Tp})^2$ $V_{SD}>V_{SG}$ & $V_{SG}>V_{Tp}$ (Saturation)
NFET or NMOS
Drain
Gate
Body
Source
$I_{DS}=0$ $V_{GS}<V_{Tn}$ (Cutoff)
$I_{DS}=k_n[(V_{GS}-V_{Tn})V_{DS}-(1/2)V_{DS}^2]$ $V_{DS}<V_{GS}$ & $V_{GS}>V_{Tn}$ (Triode/Linear)
$I_{DS}=(1/2)k_n(V_{GS}-V_{Tn})^2$ $V_{DS}>V_{GS}$ & $V_{GS}>V_{Tn}$ (Saturation)

Figure 2.8. FET long-channel current model.

expected in current, whereas the SPICE simulation using BSIM3v3 should be used to determine quantitative impacts.

The predominate wear-out/aging phenomenon of nano-meter sized ICs is BTI and Hot Carrier (HC) damage [53, 73, 22]. These aging mechanisms ultimately reduce FET drive current for the same applied terminal conditions. With less drive current, the time required for a FET to alter the subsequent gate voltage enough to cause changes in logic state increases.

The physics of all possible wear-out mechanism is not 100% understood, but the consensus is that the major impact can be modeled as an increase in threshold voltages that result in less drive current [53, 73, 22]. Using the long channel model, Figure 2.8, one can see an increase in the threshold voltages, V_{Tp} and V_{Tn}, produces less current for the same applied terminal voltages. Reduced current will produce a reduced slew rate and longer transition times for data line voltages.

The impact of reduced drive current depends upon a circuit's design. As shown in the Figure 2.6 and Figure 2.7 the result might be a reduction in amplitude and frequency of an observed harmonic. In the case of the ring oscillator sensors mentioned in Lau's work and the IBM z196 server, the operating frequency decreased [38, 74].

Despite the slower transitions, a digital circuit with built in design margins can absorb these age induced changes; correct function could be maintained as the correct line voltages are reached before a clock/decision point occurs. However, while correct function is maintained, the altered slew rate impacts URE.

An ideal digital clock signal is a perfect square wave but in reality the transitions are limited by the drive current of the transistors charging/discharging the load that is the next stage input. The previous discussion highlights the reduction in drive current and slower transitions as transistors wear-out. Figure 2.9 demonstrates the changes that slower rise and fall times have on a digital signal's higher order harmonics.

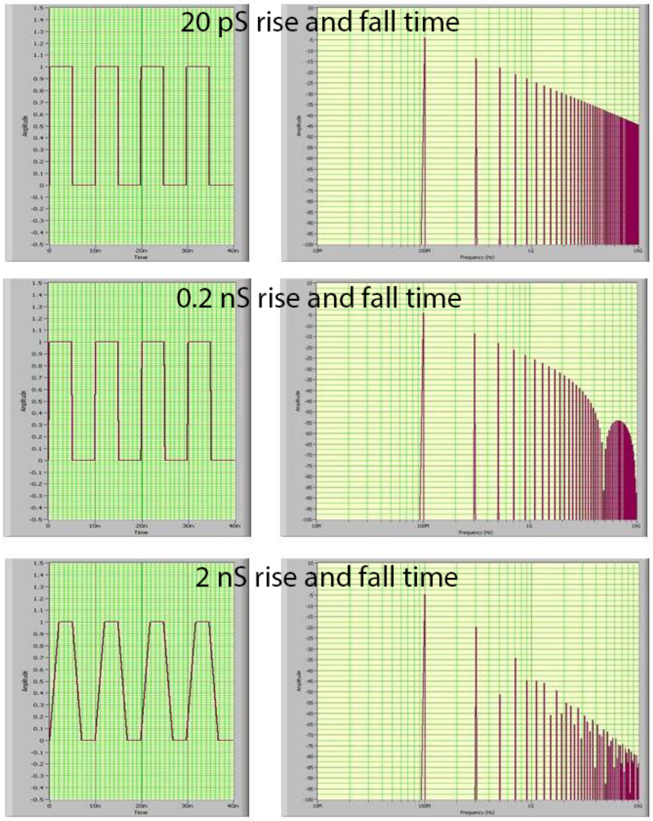


Figure 2.9. Rise and Fall Time Spectrum. Top: Spectrum for square wave with increasing rise and fall times. Left: square wave. Right: spectrum. [4]

The slower transition rates have less observed power at higher frequencies. This fact leads to one strategy for reducing EMC/EMI, design slower slew/transition rates [4, 24, 36]. However, a design margin ensuring correct function as an IC ages must allow for some measure of additional slowing. *The consumption of this design margin as an IC ages and the associated changes in the URE is the physical phenomenon that this research seeks to quantify in its impact to RF-DNA discrimination and leverage as the means to track device aging.*

2.4.3 Simulated Aging

Before conducting this research's experimental wear-out and URE signal exploitation, simulations using SPICE and changes to transistor threshold voltages was used to determine RF-DNA's ability to track circuit age. RF-DNA as applied to hardware discrimination focused on digital systems [65, 12, 15]. Many digital circuits are built from a combination of NAND gates. Staying consistent with these two facts, the simulation is based on the circuit in Figure 2.10, built entirely of two-input NAND gates.

The circuit is divided into three parts. The first part, the three voltage sources arranged vertically on the far left, are the input signals and power supply for the circuit. The center source is a Direct Current (DC) voltage source for the three NAND gates. The top and bottom sources are square-wave voltage sources that have one pico-second rise and fall times. The rise and fall times are very quick in order to simulate the two input signal that would come from off-chip input lines. The current flowing from these sources may be quite large as needed to achieve such short rise and fall times into the middle two shape inverters. The current from these two input signals is not included in the development of the current that impacts the device's URE. The timing of the square-wave input signals is arranged to exercise all four states for the 2-input NAND. The inputs count from 0-0 to 1-1 with each state lasting five nano-seconds.

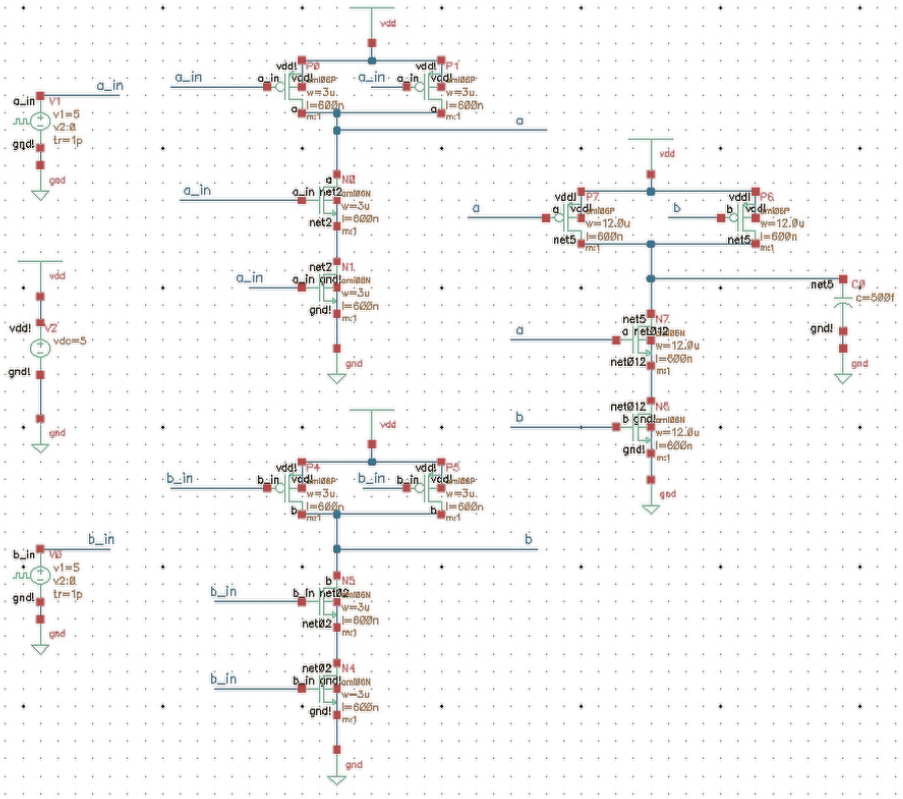


Figure 2.10. Simulated Aging Circuit with two input NAND. Middle NAND gates are two shape inverters. The right NAND gate performs 2-input NAND logic to a capacitive load.

The current from the DC voltage source is the sole current used to simulate the NAND circuit's URE. As explained in Section 2.4.1, the dominate current is the switching current flowing in the power supply runs. In this simple circuit, all switching activity that requires current from the power supply is captured at this one DC source. The derivative of the supply current was used as the input signal for the RF-DNA process. As constant current does not generate EM waves, only the change in current, the derivative was used in order to simulate the near-field URE.

The circuit's middle part consists of two shape inverters. The inverters are built using appropriately sized PMOS and NMOS transistors arranged in a 2-input NAND configuration. These NANDs shape the square-wave input signal to a realistically shaped (exponential type rise and fall) waveform. The shape inverter NANDs also serve the purpose of input pads on a real IC that drive the rest of the circuit. Each shape inverter, one for each input signal, drives the respective inputs on the 3rd part's logic NAND.

The final circuit part consists of a single two-input NAND. The transistors of the NAND gate are sized to implement a Fan Out 4 (FO-4) loading of the shape inverters. The FO-4 sizing simulates the up-sizing of transistors to drive an output signal off of a real-world IC. The final logic NAND's output is loaded with a 500 femto Farad (fF) capacitor. The 500 fF value was chosen to create realistic (slowed) rise and fall times on the logic NAND that still reached final high and low voltage values at the extremes of the un-aged and aged scenarios.

The simulation aged the circuit by altering the PMOS and NMOS threshold voltages up to a 130% of their nominal values in order to reduce every transistor's drive current thus slowing transition times. For the purpose of aging, the nominal threshold voltage magnitudes for both PMOS and NMOS was considered to be 1 Volt; actual V_{Tn} and V_{Tp} magnitudes were 0.7 and 0.9 Volts. The initial (Class-1, no threshold shift), an intermediate shift (Class-2, 115% of nominal), and full shift (Class-3, 130% of nominal), were used to train the RF-DNA MDA/ML classifier on three classes

Incremental wear-out was simulated by using ten V_T shifts from 3% to 30% added to the the un-aged V_T. All RF-DNA fingerprints associated with the ten wear-out ages where then projected onto the two dimensional space that best separated the three training classes. In addition to a mean age shift, the aged threshold shift values were allowed to vary with a Gaussian distribution with one standard deviation set to 10% of the applied mean shift. The additional Gaussian spread models the widening variation that can occur during transistor aging as not all transistors degrade at the same rate.

All transistors, whether aged or not, also had their nominal threshold voltage vary as Gaussian with one standard deviation set to 5% of the nominal, 1 Volt, threshold voltage. This 5% variation modeled the static process variation built into all transistors during manufacturing. The SPICE simulation limited all Gaussian variations to ±4 standard deviations, thus ensuring all age shifts never created a negative (net un-aging) shift. Figure 2.11 shows how the 15% and 30% wear-out ages reduced the peak current change and slew rate as the device was aged.

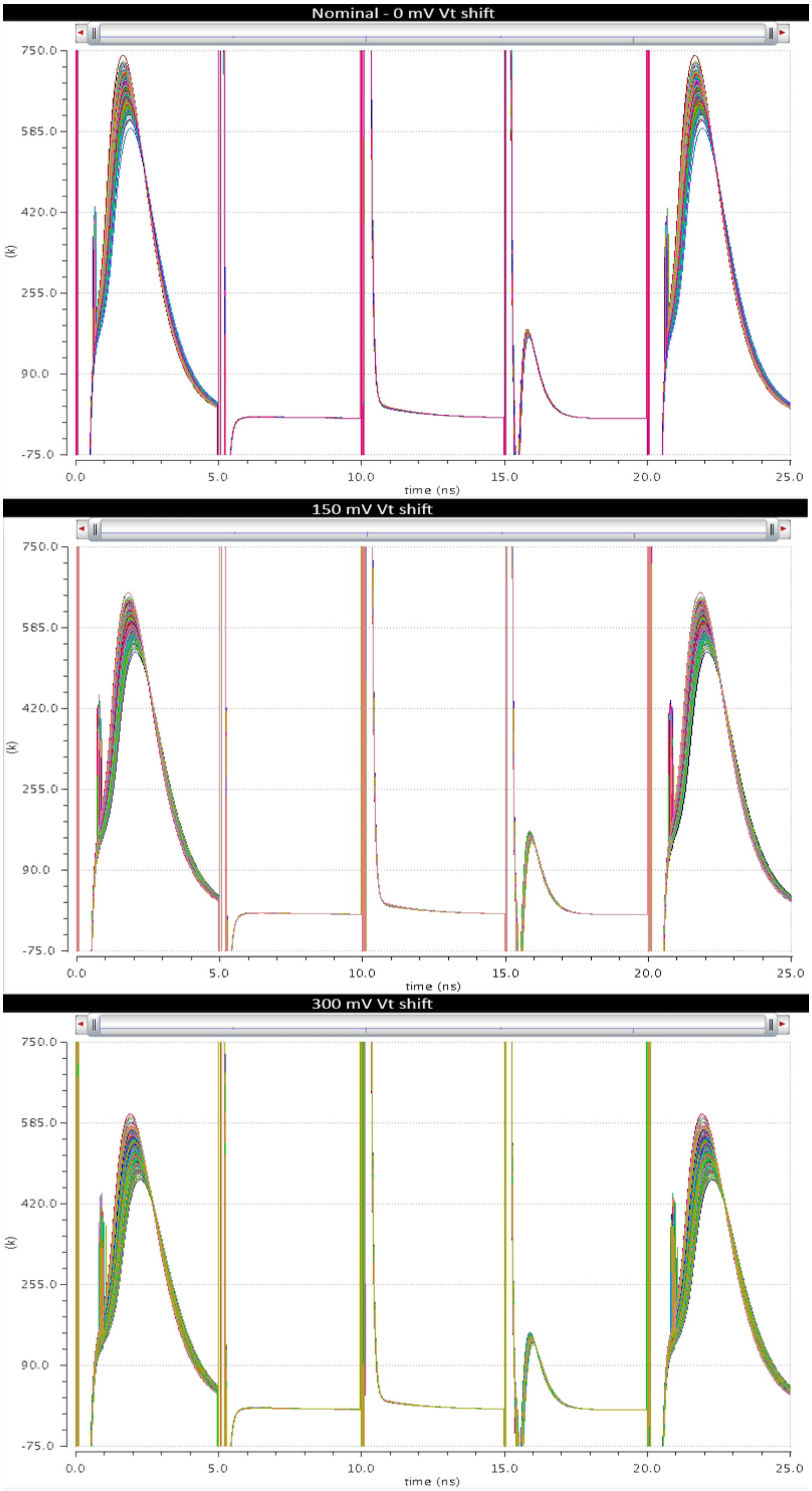
2.4.4 Combating Wear-out

Design Margin

For successive logic gates the input voltage must reach a certain values before the output can be considered correct for the input values. The minimum values at which a logic gate still provides correct output for a given input is called the noise margin [75]. The plot curves are related to voltage by Equation 2.10, where di/dt is a curve plotted in Figure 2.11.

$$i = C\frac{dV}{dt} \Rightarrow \int \frac{di}{dt} = C\frac{dV}{dt} \Rightarrow \int\int \frac{di}{dt} = C\int \frac{dV}{dt} \Rightarrow \left[\frac{1}{C}\right]\int\int \frac{di}{dt} = V \qquad (2.10)$$

Therefore, each successive age response requires more time to achieve the fixed minimum input high voltage. Using the different current responses in Figure 2.11 one can see how a design margin can account for both manufacturing process variation and wear-out changes. If the operating clock frequency is slowed the longer time required to reach the noise margin for higher ages is accomplished. This is one example of how a design margin is accomplished with de-rated clock frequency. Such an increased delay is one of the concerns that the on-chip sensor of the IBM z196 server monitors [74].



Nominal - 0 mV Vt shift

150 mV Vt shift

300 mV Vt shift

Figure 2.11. Derivative of supply current for 500 Monte Carlo runs. Top: un-aged - 0% (0 mV) V$_T$ shift. Middle: 15% (150 mV) V$_T$ shift. Bottom: 30% (300 mV) V$_T$ shift

Adaptive Circuits

The use of adaptive or redundant circuits mentioned in Section 2.3 as a means to combat PV can also be used to counteract wear-out issues. In the PV application the testing may only be conducted at the foundry during the binning process and before IC packaging. The faulty IC components can then be de-activated and spares activated before the IC is released. In the wear-out application, the same spare parts may be used but an in-situ circuit monitors IC degradation and re-configures the IC as needed.

The SSD extra word line example in Section 2.3.3 is also an example of using adaptive circuits for ensuring IC longevity. SSDs use FLASH that have limited number of write cycles. A monitoring circuit ensures all memory sub-divisions are exercised equally and can also switch in extra memory elements should some word lines cease to function due to initial PV manufacturing faults or cumulative writes [66, 28, 68].

Lifetime Estimation - Simulations and Accelerated Aging

Incorporating wear-out into design margins require knowledge of expected degradation. The binning process takes IC dies and categorizes them based on testing during the manufacturing process but only accounts for process variations [81, 56]. The information needed to create a wear-out buffer can be acquired from simulated aging and/or accelerated aging.

Simulated aging accounts for a myriad of wear-out phenomenon. Most simulators apply physics knowledge of the wear-out mechanisms and incorporates those changes into transistor model parameters [48, 79, 70]. For example, the BSSIM3vs Model used in Section 2.4.3 includes over 100 fit parameters to accurately simulate transistors. The BSIM model, and other simulation models, build their fit models by determining transistor performance to cover the spectrum of operational conditions. The spectrum of conditions can be created by stressing an actual circuit with such events as higher than normal operating temperatures and over-voltage stresses. SPICE simulation can then project wear-out performance by applying the altered model parameters. In this manner, Very Large Scale Integration (VLSI) circuits can be simulated with varying operational situations. The needed margins can then be built into the IC design and the end product can function out to the desired product lifetime.

Stressing circuits, also called accelerated aging, is not only used for determining fit model parameters but also for determine reliability, the long term product yield, of production runs. Stressing a subset of production run ICs with the purpose of determining reliability, such as Mean Time Between Failure (MTBF), leads to the bathtub curve of failure rates [21]. This bathtub curve allows manufactures to statistically estimate the MTBF for all their IC products. This estimated lifetime allows an end user to combat wear-out phenomenon by procedural actions such as replacing a part before failure rather than paying a manufacturer to build in extra precautions.

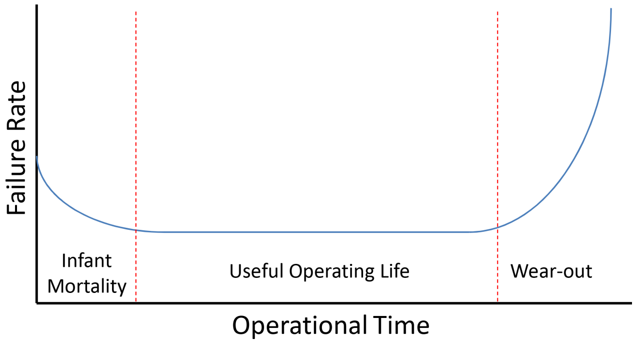


Figure 2.12. Example Bathtub Curve showing device Failure Rate versus Operational Time

An example bathtub curve shown in Figure 2.12 uses failure rates to describes three operational categories. Newly minted IC have varying levels of manufacturing induced PV. Some of the devices' PV may place their reliability right on the edge of the design margin. Short time accelerated aging stress or non-stressed operation degrades a number of devices to failure early in the lots operational lifetime, called infant mortality [75]. The majority of devices have enough design margin to absorb time induced variation during the useful (designed) operating life. At some point the devices degrade to a point exceeding the design margins and the failure rates climb above the steady state failure rate. A manufacturer may publish the warrantied lifetime out to a value below the transition to increased failure rate. The published lifetime may be significantly less than achieved in testing based on the manufactures economic decision and risks to offer guaranteed performance. Additionally, a short stress event called burn-in may be done to catch most if not all of the devices with PV that cause infant mortality [9, 57, 80].

Some devices used for application development receive little or no burn-in as the cost to perform the burn-in is not justifiable for initial development [26, 5]. The MSP430 micro-controllers used in this work were purchased as low cost developmental boards not designed for high reliability applications and likely did not undergo any significant burn-in. Should RF-DNA be able to detect changes in early operational time, RF-DNA may likewise be able to detect changes indicative of impending wear-out. None of the MSP430 devices used in this wear-out study were stressed with enough accelerated aging to force wear-out failure. Any induced wear-out changes to URE are most likely only around the transition from infant mortality to operating life described in Figure 2.12.

2.5 Wear-out Impact to RF-DNA

Sections 2.3 and 2.4 demonstrate the challenges manufacturers must overcome to ensure identical/correct function from ICs that each have unique characteristics at time of creation and over time. This section uses the SPICE simulation in Section 2.4.3 to demonstrate how simulated PV and wear-out impacts RF-DNA.

The individual steps of the RF-DNA process described in Section 2.2 were completed in the following manner. For Step-1: Signal Collection of the RF-DNA process, the entire unfiltered current derivative signals were used as the input signals. For Step-2: ROI Detection, the entire current derivate signals were used. For Step-3: Fingerprint Generation, only the amplitude signal attribute was used. The amplitude attribute signal was divided into 5 sub-regions and the total signal was used as well. No AWGN was added so all results are for a simulated as collected signal. Finally all moments were included for each of the sub-regions and the total signal.

The phase and frequency attributes were not used for two reasons. First, calculating the phase and frequency from the recorded amplitude signal requires the use of the ΔT value between each data point. The amplitude signal extracted from the SPICE simulation was designed to have a $\Delta T = 10$ pico-seconds. However, at the instant the input signals changed states (5, 10, 15, 20 pico-seconds) the simulation had non-uniform ΔT values as the simulation converged on self-consistent values during these rapid input value changes. Following SPICE converging, the desired $\Delta T = 10$ pico-seconds continued until the next change of input states. Therefore, while MATLAB could calculate phase and frequency values using a fixed ΔT value, these resulting numbers are not correct around the transitions times. Second, using phase and frequency attributes, despite the known ΔT issue, did not significantly increase the classifier accuracy.

Simulation Results / Wear-Out RF-DNA Utilization

The separation between current derivative plots in Figure 2.11 can be clearly seen by human inspection as a drop in peak value and a widening of each curve. This separation produces MDA/ML results of Figures 2.13 and 2.14. Figure 2.13 show MDA/ML classification separability of the un-aged (0 V shift), middle age (150 mV shift) and full age (300 mV shift) events. The un-aged class (blue dots) have some variation due to the 5% allowed process variation. The middle-age class (green dots), added a 150 mV age shift with 10% standard deviation. The full-age class (red dots) added a 300 mV shift with 10% standard deviation. The intentional overlap of the current derivative signal results in overlap in the projected space.

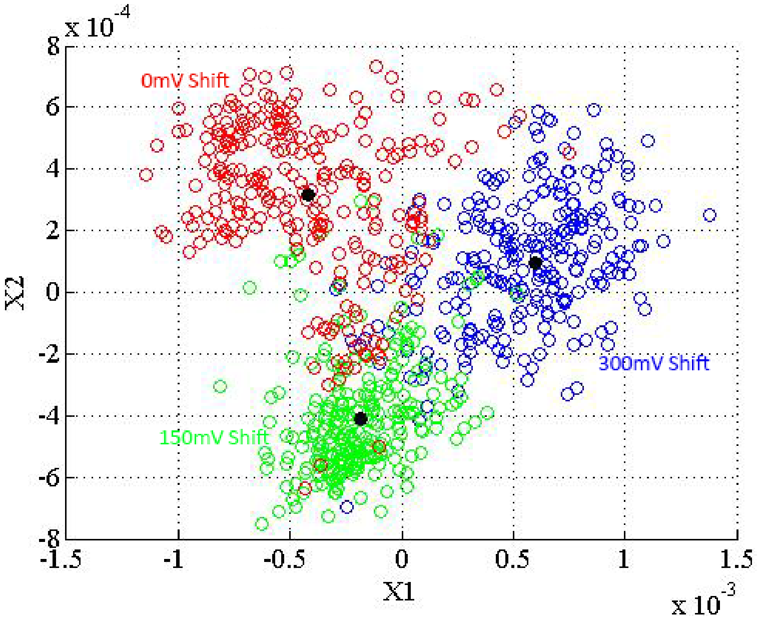


Figure 2.13. MDA Projection of Aged/V$_T$-shifted Classes. Separation of the three classes is visually discernible.

Figure 2.14 records the ROC results. In this case, all three different ages were separable with greater than 10% EER. The 1:1 designator in the legend, indicates all ages that were not Class-1 were almost never called Class-1 by the MDA/ML model. Likewise, the 2:2 and 3:3 indicate false verification rates were also below the 10% EER benchmark.

In real-world IC circuits the collected URE signals will not be as neat as the current derivative simulation. In this simulation the modeled wear-out for each transistor directly impacted the RF-DNA collection signal. In the case of the MSP430 micro-controller some transistors may undergo wear-out degradation and others may not display any degradation. The URE from the micro-controller is then a combination

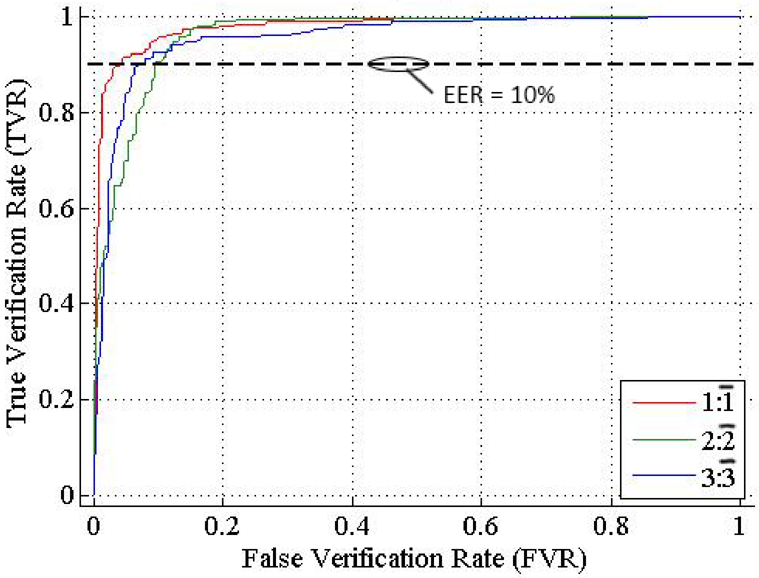


Figure 2.14. MDA Separability of Aged/V$_T$-shifted Classes: 0 mV shift - Red, 150 mV shift - Green, 300 mV shift - Blue.

of all IC current from all transistors each degrading at different rates. The resulting wear-out URE may not be separable by human inspection. However, if some changes do manifest in the collected URE, the MDA/ML machine learning techniques will hopefully detect the wear-out artifacts. In this effort wear-out artifacts are observed and discussed in Chapter IV.

The remaining sections of this document, will apply the MDA/ML machine learning using aged MSP430 micro-controllers to determine if such changes are detectable and usable to accomplish the three goals listed in Section 1.4: *Device Discrimination*, *Age Estimation*, *Age Discrimination.*

III. Methodology

This chapter describes the methods used to age (force wear-out), collect URE signals, train the MDA/ML machine learning, and how the results of each of the three wear-out goals will be presented in Chapter IV. Because some methods change for each of the three wear-out goals (*Device Discrimination, Age Estimation, and Age Discrimination*) this chapter first describes topics that are universal to all three goals. The universal methods encompass the first three steps of the RF-DNA process described in Section 2.2. The sections that are goal specific include the last steps of the RF-DNA process. These sections also discuss the results presentation format as they differ for each goal.

3.1 Universal Methods

3.1.1 Test Device Selection

Texas Instruments MSP-EXP430F5529LP developmental board micro-controllers, shown in Figure 3.15, were chosen as the test devices. The MSP430 architecture is a single core 16-bit multi-cycle RISC device [69]. The MSP430 does not offer parallel processing (hyper-threading) and enables explicit control over all device operations. With exact operational control, the software influence on URE can be maintained as a constant for all collections. Therefore any alterations to URE can be attributed to hardware changes.

3.1.2 Testbed Hardware Configuration

This research utilized a signal collection setup similar to previous URE collections [65, 15]. Figure 3.16 shows the collection set-up for this wear-out study. All signal collections for all three research goals were conducted in the same testbed.

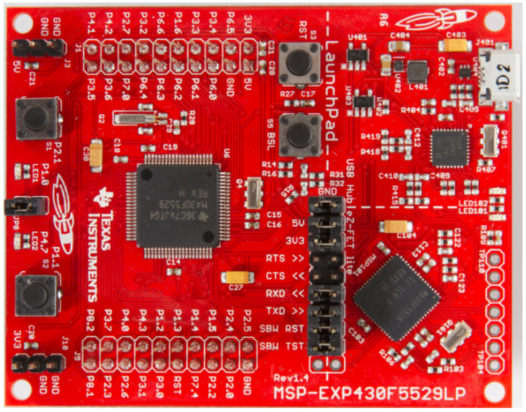


Figure 3.15. Texas Instruments MSP-EXP430F5529LP Development Board

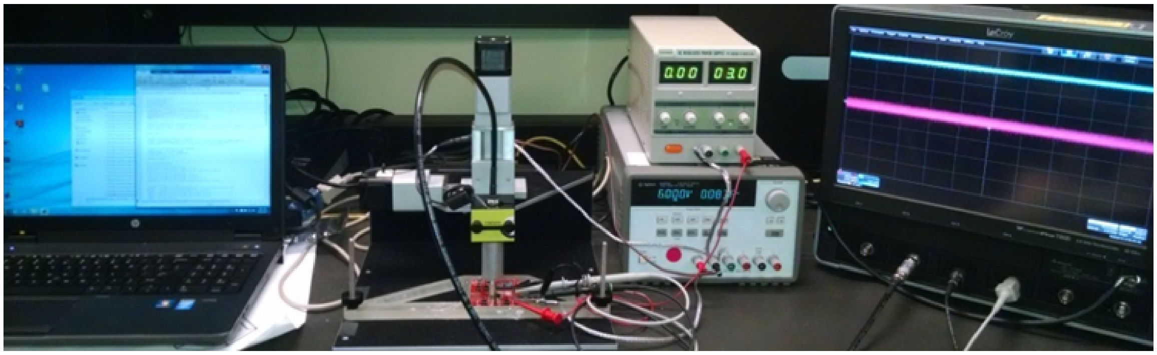


Figure 3.16. Signal Collection Testbed. Far-Left: MATLAB laptop control. Center-Left: Near-field EM probe and Test Device. Center-Right: Regulated Power Supplies. Far-Right: Oscilloscope.

The testbed included a computer running MATLAB code to control the EM probe location via a motorized table. MATLAB also controlled the setup options for the oscilloscope. Regulated power supplies powered the EM probe and test device. An oscilloscope sampled and stored the near-field emissions detected by the EM probe. The near-field signals collected by a Riscure206HS RF-probe were captured by a LeCroy WaveMaster 804Zi oscilloscope. The oscilloscope, power supplies, and MSP430 test device were all connect to each other via a common ground using a flattened coax braid grounding strap. The near-field probe was connected to the oscilloscope through an in-line anti-aliasing LPF via a 50 Ohm coax cable.

The MSP430 micro-controllers operated with default clock speed at approximately

1 MHz. The testbed oversampled at 2.5 GSps using an in-line 520 MHz LPF. A 520 MHz LPF was used rather than a typical 1.25 GHz anti-aliasing value because of observed noise on oscilloscope signals above 520 MHz. Additionally, the loss of bandwidth from 520 MHz to 1 GHz was not a problem due to subsequent MATLAB filtering with a Band Pass Filter (BPF) with a passband between [1 - 250] MHz. The MATLAB BPF purpose is explained in Section 3.1.6. Figure 3.17 displays the passband of the anti-aliasing filter with $f_{-3dB} = 575$ MHz. After all time domain oscilloscope signals were saved, no additional hardware was required. All subsequent signal processing and analysis was accomplished in MATLAB.

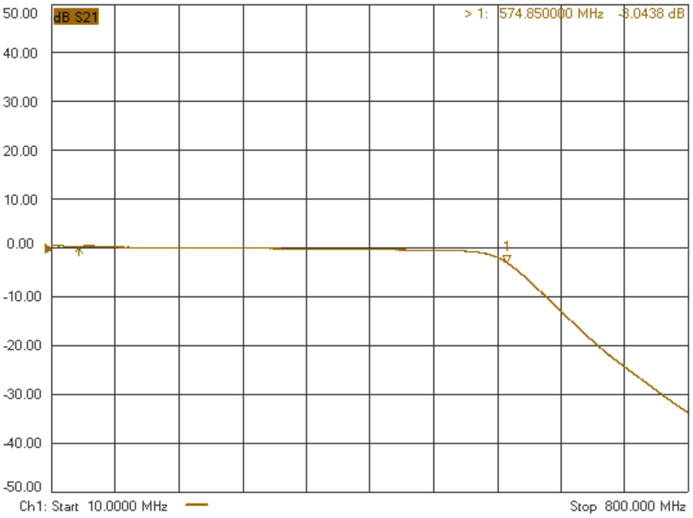


Figure 3.17. DC-520MHz Anti-alias LPF Passband. Actual -3 dB point at 575 MHz.

The actual IC used for near-field collection is the largest square IC package centered on the Printed Circuit Board (PCB) as shown in Figure 3.15 and Figure 3.18. Once the operational code was programed on the micro-controller all developmental board components other then the MSP430 micro-controller and necessary support hardware were disabled by removing the associated power jumpers. During testbed operations the MSP430 was powered using a regulated power supply via the battery DC pins at 3V nominal voltage as if operating from two AA batteries.

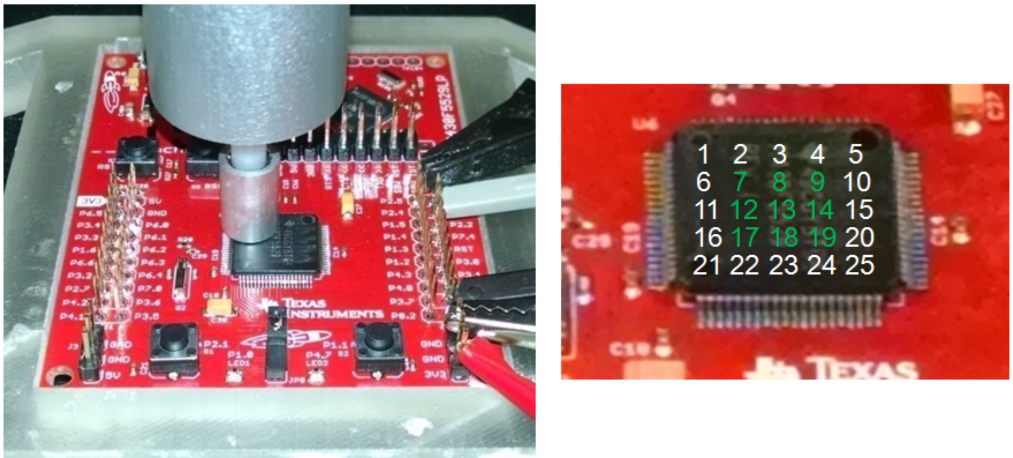


Figure 3.18. EM probe placement (left) and collection locations (right) across the test device. Central locations identified with green numbers.

The X-Y table was used to move the RF-probe to 25 locations across the surface of the MSP430. The 25 equally spaced locations were arranged in a 5-by-5 grid from edge to edge of the DUT as shown in Figure 3.18. The number of locations was chosen in order to provide some measure of locality but limit raw data storage requirements. Collections at multiple locations were needed in order to improve the chance of capturing changes due to aging. The underlying IC die layout and packaging configuration was not know and age induced changes may be localized to specific areas of the IC. For all collections the RF shield on the Riscure probe was in the lowest possible position to limit any URE cross contamination between the locations on the 5-by-5 grid. The central probe locations, (7, 8, 9, 12, 13, 14, 17, 18, 19 - indicated with green numbers), were used for multi-location fingerprints when RF-DNA operated with multi-location fingerprints versus a single-location device fingerprints. The central nine were used versus locations around the package perimeter in order to focus the near-field probe beam-width on URE emanating from the IC die. Device dies are typically physically centered in the packaging.

The MSP430s performed a 128-bit Advanced Encryption Standard (AES) sequence implemented with software code. Once the encryption was completed on a data block, the sequence was re-accomplished with the same data block. The AES sequence was ran in a continuous loop. Since the unencrypted data block never changed, the encryption result was always verified against the known correct result at the end of each loop. A development board light was used to indicate if the AES code ever failed to correctly encrypt the data. The failed encryption indicator had no means to be reset except through removal of device power. This check was used to determine if the hardware ever failed to correctly operate throughout the entire accelerated aging oven sequence. Failed encryption was never indicated throughout the entire wear-out process. The AES code is included in Appendix A: AES Code.

3.1.3 Collected Signal Specifics

The near-field probe signal, MSP430 main clock, and a trigger signal were collected, sampled and digitally stored for each of the 25 locations. The RF-probe is the main interest signal and 900 traces were recorded for each location per device per age. The trigger signal was used to align collected emissions from the same segment of code for all 900 traces. The trigger signal was set to go high just before the AES code entered the encryption routine. The trigger trace was only recorded once for each location. The clock signal was also only saved once per location. Figure 3.19 shows an example signal capture containing 2.5 of the 10 AES encryption rounds. The densely packed data points at the $t = 0, 2, 4$ milli-second locations are each the start of an AES round.

The signals used for the wear-out studies only saved URE traces for 100 micro-seconds after the trigger signal indicated the start to the AES encryption code. The MSP430's average number of clock cycles per operation is four clocks per operation. The 100 micro-second recording length was chosen to capture a signal equivalent to at least 20 average operations - 80 clock cycles. Additionally, the first 500 oscilloscope

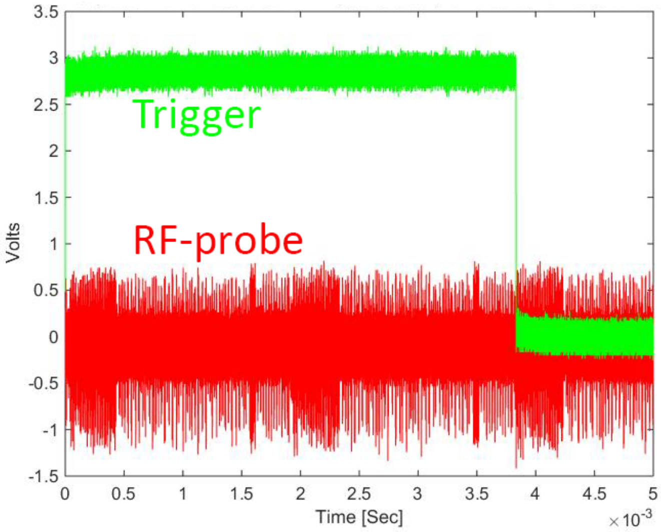


Figure 3.19. Raw Riscure EM Probe Trace.

recorded data points were removed from all traces because of the spike in near-field probe collection related to the current surge from the trigger line. Five-hundred data points equates to 200 nano-seconds with the 2.5 GSps sampling rate. The 500 removed data points eliminate about one fifth of a clock cycle. Figure 3.20 illustrates the near-field URE probe traces are dominated by the spikes in current related to transistor switching activity at each clock transition.

Ideally, the 2.5 GHz sampling rate would be set higher in order to capture the smallest signal change nuances due to wear-out. However, with 900 collections for each of the 25 locations, a planned 12 MSP430 boards, and nine planned age increments, the total data storage requirement and time to capture the signals set a practical limit on the sampling rate. Each age increment collection had to be completed in 24 hours as the next MSP430 boards in sequence required collection the next day. The collection sequence is explained in Section 3.1.5: Incremental Aging & Signal Collection.

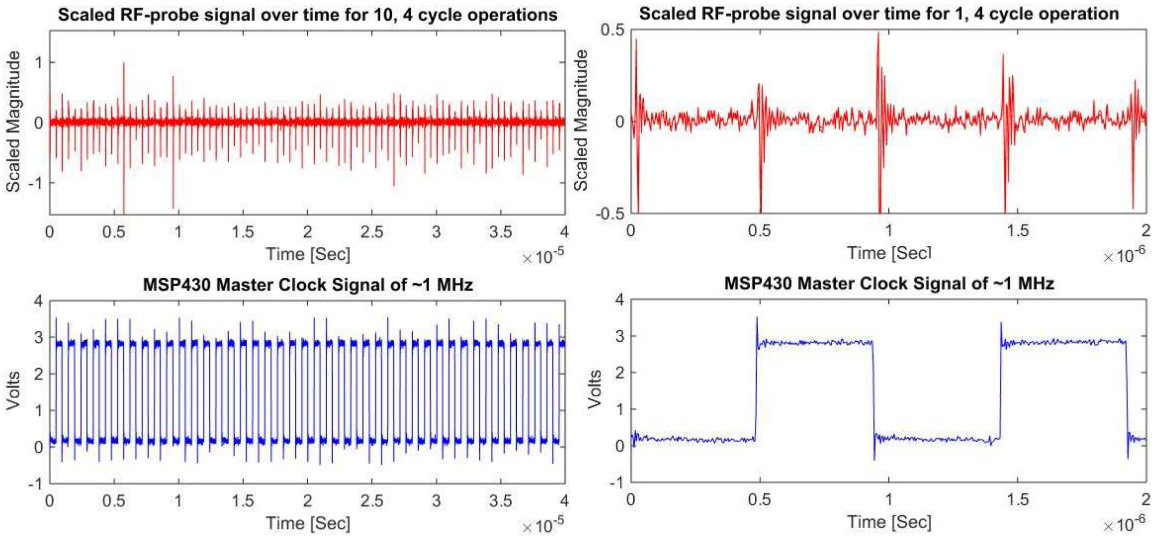


Figure 3.20. Scaled Riscure RF-Probe and Clock Signals. Left plots span 40 μSeconds, Right plots span 0 - 2 μSeconds.

3.1.4 Accelerated Aging Stress

Operating a DUT at a higher than normal ambient temperature is one common semiconductor industry method to induce wear-out in accelerated time-frames [17, 27]. This method, called High Temperature Operating Life (HTOL), operates a sample of DUTs at a temperature exceeding normal operating conditions for an extended time. The percentage of devices that fail is then used to determine the reliability of the part. This technique was used to accelerate device wear-out in this research.

MSP430 devices were aged by running the AES code while holding them at oven temp $T_{oven} = 110°\mathrm{C}$ with 10% over-volt stress by powering with 3.3 VDC. However, the digital core logic is regulated down to 1.8 Volts by the MSP430 development board [6]. Therefore, the over-volt stress may not induce any wear-out effects. The boards were allowed to heat from room temp to T_{oven} at a rate of 3.5°C/min (approximately 30 minutes), held at 110°C for 22 hours, and then cooled back to 25°C at a rate of 3°C/min. Gradual temperature changes were employed to minimize thermal cycling impacts to packaging wire bonds and packaging materials and optimize URE changes due to transistor wear-out. Accelerated aging designed to impact packaging and wire bonding typically employee temperature cycling rates of 5°C/second [77, 41]. After cooling the devices were held at 25°C in the oven until they were removed for signal collection. Temperature during signal collection was not strictly controlled, but was mainted at the ambient temperature ($T_{ambient} = 24°C$) of the office room environmental control system housing the URE collection testbed. MSP430 power was temporarily removed during the transfer of devices from the oven to collection testbed. Power was also temporarily removed during transfer from the collection testbed to the power station maintaining AES operation at $T_{ambient}$ in the same office room housing the collection testbed. Device power during signal collection, and resting operation between oven aging and collection events was maintained at the nominal developmental board specification of 3.0 VDC.

The accelerated age temp, $T_{oven} = 100°C$ was chosen to stress the MSP430 over their published ambient operational limit ($T_{max} = 85°C$) by the same 25°C over-temp used in the EMC work mentioned in Section 2.4.1. The T_{oven} value was also chosen to stay below the failure limits of the PCB [69, 20, 6].

3.1.5 Incremental Aging & Signal Collection

A total of 16 MSP430 devices were ultimately used in this study. The 16 devices were grouped into three broad categories and the nomenclature for all devices used a two character alpha-numeric code. The first character (A, B, C, D, E) indicates the device's broad category. The second character (1, 2, 3, 4) indicates which device was used in the broad category. The number-4 has an additional meaning; such devices where never oven aged and serve as control device to validate the RF-DNA testing. Table 3.1 provides the meaning of each alphanumeric designator. The different attributes for the device categories exist to test the three RF-DNA goals (*Device*

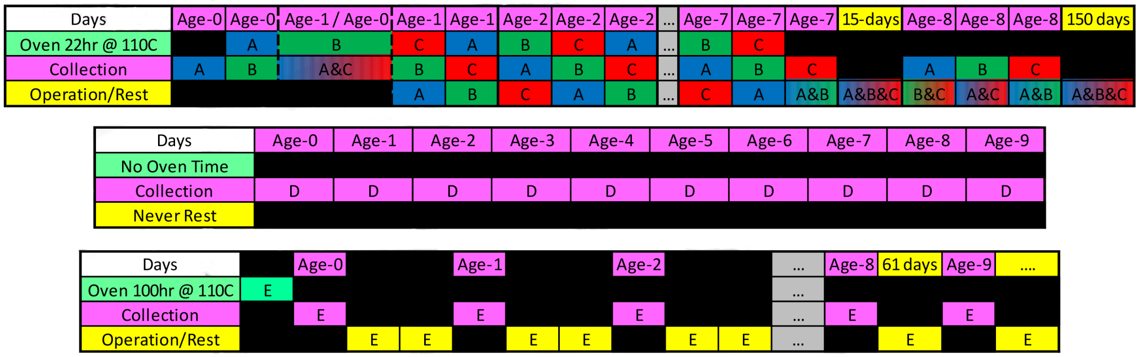
Discrimination, Age Estimation, Age Discrimination) as explained in Sections 3.2 - 3.4.

Table 3.1. Alphanumeric Designator Meaning

Device Group -- A, B, C: 4 per group, D & E: 2 per group					
	A	**B**	**C**	**D**	**E**
Always on except for transfer	A1 - A4	B1 - B4	C1 - C4	No	E1, E2
Only on during signal collection	No	No	No	D1, D2	No
Incremental Oven Aging	A1, A2, A3	B1, B2, B3	C1, C2, C3	No	No
No Oven Aging	A4	B4	C4	D1, D2	E1, E2
Oven Burn-In	No	No	No	No	E1, E2
3-day cycle between collections	A1-A4	B1-B4	C1-C4	No	E1-E2

The three different broad categories related to the three different age-collection sequences as shown in the three divisions of Table 3.2. The top region relates to the A-B-C device sequence. The middle region is for the D device sequence. The bottom region describes the E device sequence.

Table 3.2. Collection Sequence: Top - A-B-C Devices; Middle - D Devices; Bottom - E Devices.



Days	Age-0	Age-0	Age-1 / Age-0	Age-1	Age-1	Age-2	Age-2	Age-2	...	Age-7	Age-7	Age-7	15-days	Age-8	Age-8	Age-8	150 days
Oven 22hr @ 110C		A	B	C	A	B	C	A	...	B	C						
Collection	A	B	A&C	B	C	A	B	C	...	A	B	C		A	B	C	
Operation/Rest				A	B	C	A	B	...	C	A	A&B	A&B&C	B&C	A&C	A&B	A&B&C

Days	Age-0	Age-1	Age-2	Age-3	Age-4	Age-5	Age-6	Age-7	Age-8	Age-9
No Oven Time										
Collection	D	D	D	D	D	D	D	D	D	D
Never Rest										

Days		Age-0			Age-1			Age-2			...	Age-8	61 days	Age-9	....
Oven 100hr @ 110C	E										...				
Collection		E			E			E			...	E		E	
Operation/Rest			E	E		E	E		E	E	...		E		E

The first of the three broad categories includes the A, B, C devices, 12 in total: A1-A4, B1-B4, C1-C4. The A-B-C group are in collections of four devices 1 - 4. The A4, B4, C4 devices were never oven aged but continuously ran the AES code with the same number of operating hours as the 1-3 devices. The 1-3 devices were oven aged in nine increments and while the total run time is the same as the A4, B4, C4 devices, the run time included hours at the $T_{oven} = 100°\text{C}$ oven temperature. Across the A, B, C groups the 1 - 4 devices were identically operated with AES always running with the similar down time due to transfer between collection testbed and rest status (continuous operation at $T_{ambient} = 24°\text{C}$ ambient temperature with 3 VDC). The operation conditions were different between the 1-3 and 4 devices as the 1-3 devices were over-volt stressed, over-temp stressed and the down time during transfer was longer. The transfer time for the 1-3 devices was longer since the oven was not co-located in the same office room housing the collection testbed. The additional break down into A, B, C groups was required because the oven used to accelerate device wear-out could only fit three MSP430 developmental boards at one time.

The collection sequence for the A-B-C device followed a 3-day cycle due to oven size limitations and to obtain the aged collections in the shortest amount of time. The initial un-aged (Age-0) collections were overlapped and the Age-0 to Age-1 cumulative run time was only 2-days to ensure the same 3-day gap between subsequent ages from Age-1 and greater. The following example provides the details of the sequence. In Table 3.2 using the top sequence, take the 24 hours (22 hours at temp plus the ramp-up and ramp-down time) labeled as Age-1 just to the right of the dashed vertical line. In this day, C1-C3 are in the oven for their first 24-hr aging cycle. B1-B4 collections for Age-1 are being conducted after their first oven aging event: B1-B3 stressed in the oven and the equivalent total run time for B4. A1-A4 are in rest status running AES code at ambient temperature, following A1-A4 collections the previous day. The next day C1-C3 are removed from the oven, and the Age-1 collections for C1-C4 occur. When the C1-C3 devices are removed from the oven, the A1-A3 devices previously in rest status are placed in the oven for the stress to move them to the Age-2 state. B1-B4, are now in rest operational state.

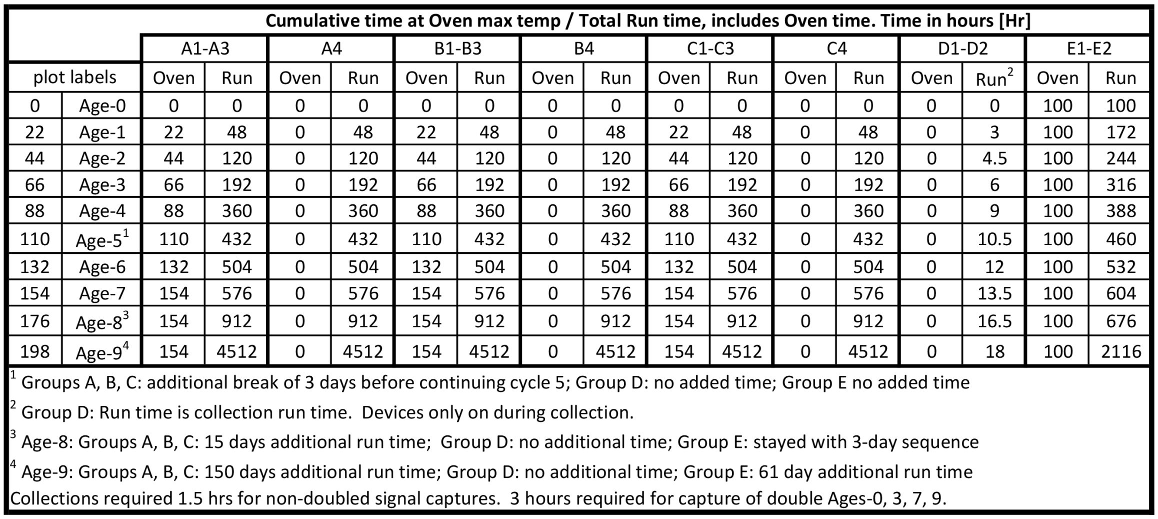
The D category, with two devices D1 and D2, was added to the data set after the original control devices (A4, B4, C4) displayed some age based separability in initial data analysis. A4, B4, C4 while not oven aged were maintained in continuous operation during the incremental 3-day aging and collection sequences. The 3-day sequences required a month to complete. The incremental collections of the 4-devices may have some wear-out differences due to a month of operation. The D group did not allow the devices to operate in rest status between incremental URE collections. D1 and D2 were only powered on during signal collections. The collections were again labeled as Age-0, Age-1, ..., Age-9 but had no oven-time nor rest aging time. Because no rest time was allowed, each labeled age collection occurred over 9 consecutive days. The middle sequence of Table 3.2 shows the D-device sequence in the same format used to describe the A-B-C collection sequence.

The E category, with two devices E1 and E2, was added as an additional type of control device. The E-devices underwent 100 hours of continuous burn-in at 110°C for 100 hours with the 3.3 VDC over-volt stress just like the A-B-C device's 22-hr accelerated aging stress. However, after the initial burn-in, E1 and E2 never received additional oven time. E1 and E2 did follow the continuous operation time similar to the A4, B4, C4 devices and therefore followed a 3-day collection sequence as shown in the bottom sequence of Table 3.2.

Age-8 and Age-9 for all devices were modified from the 3-day sequence covering Age-0 to Age-7. Age-8 did not receive any additional oven time over Age-7. Age-9 did not receive any additional oven time over Age-8. Age-8 instead was collected after the devices were continuously operated (rest status) at ambient for 15 days. Age-9 was collected after the devices were in rest stats after 150 additional days. The D1, D2 collection were done after the same 15 and 150 day delays but Age-8 and Age-9 for D1 and D2 did not have addition rest status hours since these devices were only powered during URE collections. Thus the Age-8/9 collections as shown in the middle sequence of Table 3.2 do not indicate the 15 nor 150 day gap.

With the different collection sequences, each device category accounts for different cumulative operational run time and cumulative wear-out. Table 3.3 lists the different cumulative times for all devices.

Table 3.3. Cumulative Device Run Times



		Cumulative time at Oven max temp / Total Run time, includes Oven time. Time in hours [Hr]															
		A1-A3		A4		B1-B3		B4		C1-C3		C4		D1-D2		E1-E2	
plot labels		Oven	Run	Oven	Run	Oven	Run	Oven	Run	Oven	Run	Oven	Run	Oven	Run[2]	Oven	Run
0	Age-0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	100	100
22	Age-1	22	48	0	48	22	48	0	48	22	48	0	48	0	3	100	172
44	Age-2	44	120	0	120	44	120	0	120	44	120	0	120	0	4.5	100	244
66	Age-3	66	192	0	192	66	192	0	192	66	192	0	192	0	6	100	316
88	Age-4	88	360	0	360	88	360	0	360	88	360	0	360	0	9	100	388
110	Age-5[1]	110	432	0	432	110	432	0	432	110	432	0	432	0	10.5	100	460
132	Age-6	132	504	0	504	132	504	0	504	132	504	0	504	0	12	100	532
154	Age-7	154	576	0	576	154	576	0	576	154	576	0	576	0	13.5	100	604
176	Age-8[3]	154	912	0	912	154	912	0	912	154	912	0	912	0	16.5	100	676
198	Age-9[4]	154	4512	0	4512	154	4512	0	4512	154	4512	0	4512	0	18	100	2116

[1] Groups A, B, C: additional break of 3 days before continuing cycle 5; Group D: no added time; Group E no added time

[2] Group D: Run time is collection run time. Devices only on during collection.

[3] Age-8: Groups A, B, C: 15 days additional run time; Group D: no additional time; Group E: stayed with 3-day sequence

[4] Age-9: Groups A, B, C: 150 days additional run time; Group D: no additional time; Group E: 61 day additional run time

Collections required 1.5 hrs for non-doubled signal captures. 3 hours required for capture of double Ages-0, 3, 7, 9.

The 900 bursts collected for each age were obtained by combining 3 reposition sets of 300 burst per set. Between the 300 burst sets, the DUT was fully removed from the testbed jig and repositioned in the jig as shown in Figure 3.21. Previous URE collections demonstrated URE signal's high sensitivity to reposition errors as mentioned in Section 2.2.1 [65]. Because all devices had to be removed from the collection testbed in-order to conduct the oven aging events, each collection may demonstrate changes in URE due to reposition miss-alignment.

The three ages used for MDA/ML class training based on age (Age-0, Age-3, Age-7) recorded two sets of 900 trace signals for a total of 1800 signal bursts. Nine-hundred of the 1800 were used for the MDA/ML training steps. The extra 900 bursts were

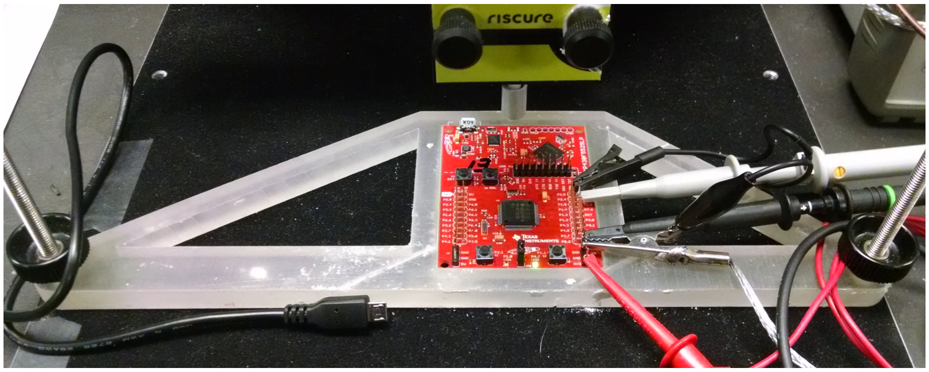


Figure 3.21. Physical Repositioning Jig used to minimize DUT misalignment between age set signal collections

then used as independent signals, separate from training, for testing/use to determine accuracy of this research's techniques.

During initial analysis the Age-9 (4512 cumulative run hours for A-B-C devices, 2126 cumulative run hours for E1/E2, 18 cumulative run hours for D1//D2) presented results inconsistent with expected outcomes. The 2-norms of all fingerprints for all ages and repositions using devices C1, C4, D1, and E1 are plotted in Figure 3.22. The black clusters show the clustering of fingerprints at the 10 different ages and the 3 repositioning sets for each age. The last age cluster for each of the four devices are the 2-norms for the Age-9 URE signal collections. C1, C4, and E1 all were operating in the rest state for roughly six and three months respectively imparting a large operating time jump between Age-8 and Age-9. The D1 Age-9 cumulative run time jump is no different than the operation time jump from Age-7 to Age-8; the D devices were only on during signal collection. The D1 Age-9 fingerprint 2-norms should not show a similar shift to the other devices if the dominant difference between Age-8 and Age-9 is due to cumulative run time.

All Age-9 signal collections were completed after the testbed components were utilized by other research efforts and personnel. It is possible the re-utilization altered the testbed imparting the D1 shift. Because of this unexpected shift in D1, the Age-9

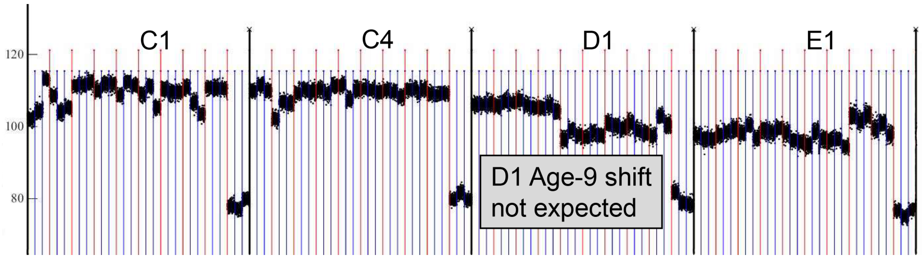


Figure 3.22. 2-Norm of Fingerprints. Blue line division signify reposition sets. Red line divisions signify Age set. Black line divisions signify Device changes. Unexpected Age-9 shift for D1 device similar to other devices operating in rest status.

data was not used for any of the three RF-DNA goals.

3.1.6 Collected Signal Filtering

Age Estimation was attempted before the other two goals because it was the viewed as the most difficult challenge and the best environment to discover new techniques to best capture wear-out induced variation. While the actions were completed during the efforts for *Age Estimation*, theses actions apply to all research goals and therefore the methods are describe in this Universal Methods Section 3.1. Filtering described here includes traditional concepts of Notch and Bandpass filters but also includes signal manipulation that increases machine learning performance, e.g. removing parts of the collected signal that either provide no classifier enhancement or degrade performance, thus improving the effective SNR.

Notch and Bandpass Filter

The following filtering was applied to all signals for all three research goals. A MATLAB software implemented 1-250 MHz bandpass filter removed any DC bias from the collection testbed. The 250 MHz cutoff was chosen after observing a subset of all normalized Power Spectral Density (PSD) plots where signal content appeared to have less importance relative to the greater PSD response below 250 MHz. Notch filters were also applied via MATLAB code at 196.5, 208, and 224 MHz to remove PSD spikes. These spikes appeared as testbed collection artifacts and were remove to ensure the normalized Fast Fourier Transform (FFT) had peak values at similar frequencies when comparing Age-0 and Age-7 collections.

Figure 3.23 displays the normalized impulse response for all MATLAB filtering. The top-right subplot show the response of the bandpass filter used primarily to remove any DC bias, while still passing the frequencies at and above the MSP430 clock frequency, approximately 1 MHz. The three remaining subplots document the notch filtering attenuation.

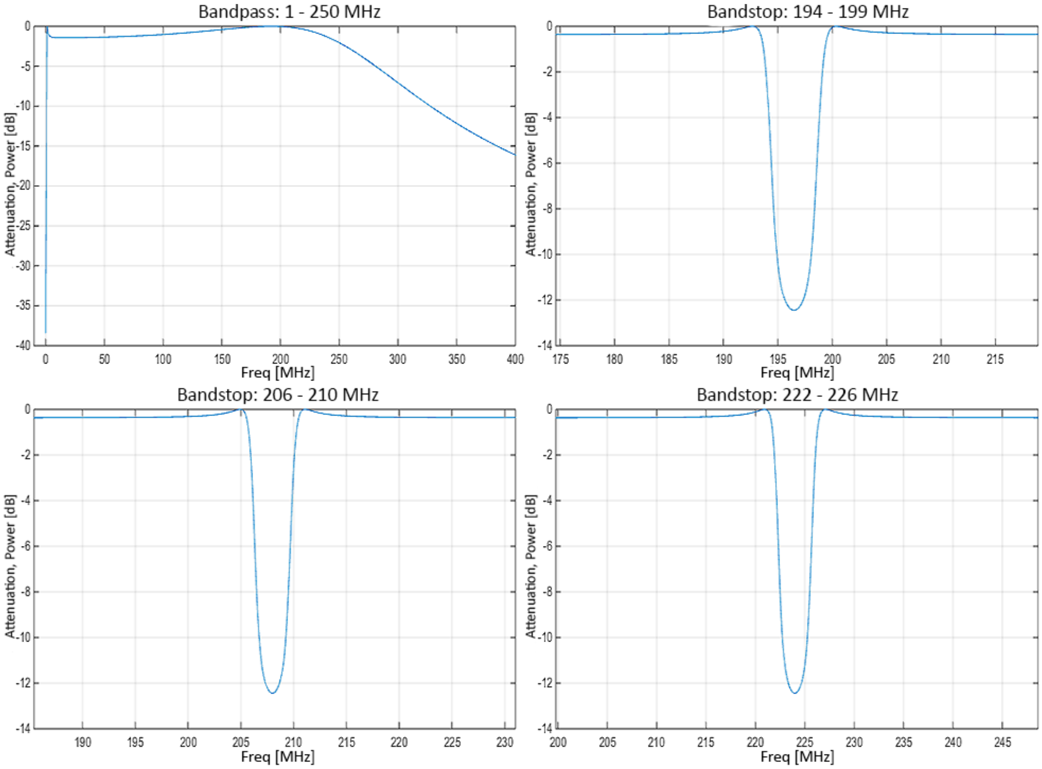


Figure 3.23. Normalized impulse response for Bandpass and Bandstop MATLAB filters.

Figure 3.24 displays an example of altered PSD changes between Age-9 and Age-0 responses used to identify candidate locations, described in the next subsection: Single versus Multi-locations.

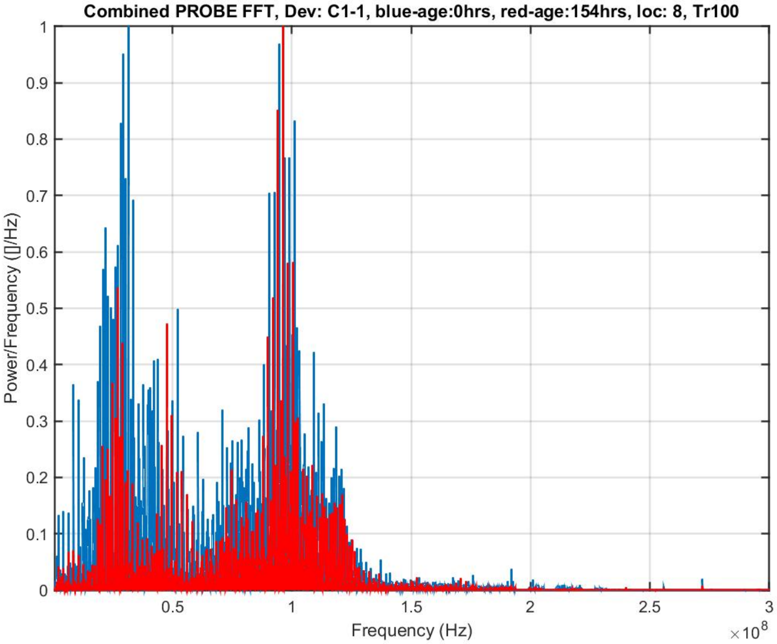


Figure 3.24. Normalized & Filtered (Bandpass 1-250 MHz, Notch at 196.5, 208, 224 MHz) PSD for a single URE burst using device C1 at package location-8. Compares URE at Age-0 (blue/dark-grey plot) to the URE at Age-7 (red/light-grey plot).

Single versus Multi-locations

Because wear-out impacts transistor switching current and the EMC study in Seciton 2.4.1 showed wear-out altered the spectrum of emissions, PSD changes were used to identify candidate locations showing wear-out artifacts as differences in PSD between the max training age (Age-7) and the un-aged (Age-0) response. The PSD was also used to improve the signals passed to the fingerprint generation step of RF-DNA. Figure 3.24 plots the normalize FFT for a single device at the same location comparing the PSD for the max training age to the un-aged URE collection.

The *age estimation* efforts, applied candidate locations identified for a few devices and used those locations for all devices. Using the single candidate locations across the multitude of devices produced inconsistent performance. As a result, the attempt to identify specific locations that are more prone to wear-out was abandoned. Instead fingerprints were generated using multiple locations. The locations chosen were the nine central locations shown in Figure 3.18 in Section 3.1.2.

3.1.7 Fingerprint Generation

Fingerprint Features

Using nine locations required changes in the way the URE collections were divided into the fingerprint generation subregions. When single locations were used fingerprint generation divided the signal burst into 20 uniformly spaced subregions. Each subregions roughly aligned with four clock cycles (a single average operation length). Using all signal attributes and all moments, described in Section 2.2.3, for the 20 subregions and the entire signal resulted in fingerprints with 252 features. Using the same division with nine locations would create fingerprints with 2,268 features. Because MDA/ML determines eigenvectors that best create the separation hyperplane, described in Section 2.2.4, the number of features within each fingerprint must be less than or equal to the number of fingerprints used to train the MDA/ML model. With 900 collected burst and half (450) used to develop the MDA/ML model, the number of fingerprint features must be less than or equal to 450.

To limit fingerprint features at or below 450, the changes in average feature values for all the central locations, signal attributes, and moments were observed between Age-0 and Age-7 fingerprints. The greatest change was observed from the Kurtosis, Skewness, and Variance values calculated from the URE's instantaneous amplitude. Using Kurtosis, Skewness and Variance of the amplitude attribute provided 432 features with 16 sub-regions without the moments for the entire signal. Selection of these fingerprint features was done without any classifier training using only the average of all fingerprint values and these are therefore applicable to any future classifier training that intends to document or use wear-out differences.

Subregion: uniform versus clock transitions

The change from 20 to 16 subregions was required to obtain feature numbers below 450. This switch also altered how the sub-regions are extracted from the URE signal burst. Fingerprints with 20 subregions were uniformly spaced and each region roughly included the signal spanning four clock cycles. The 16 subregions employed windows centered around each URE signal spike associated with clock transitions. Figure 3.25 provides a visual reference for defining the 16 subregions with the URE spikes at each clock transition.

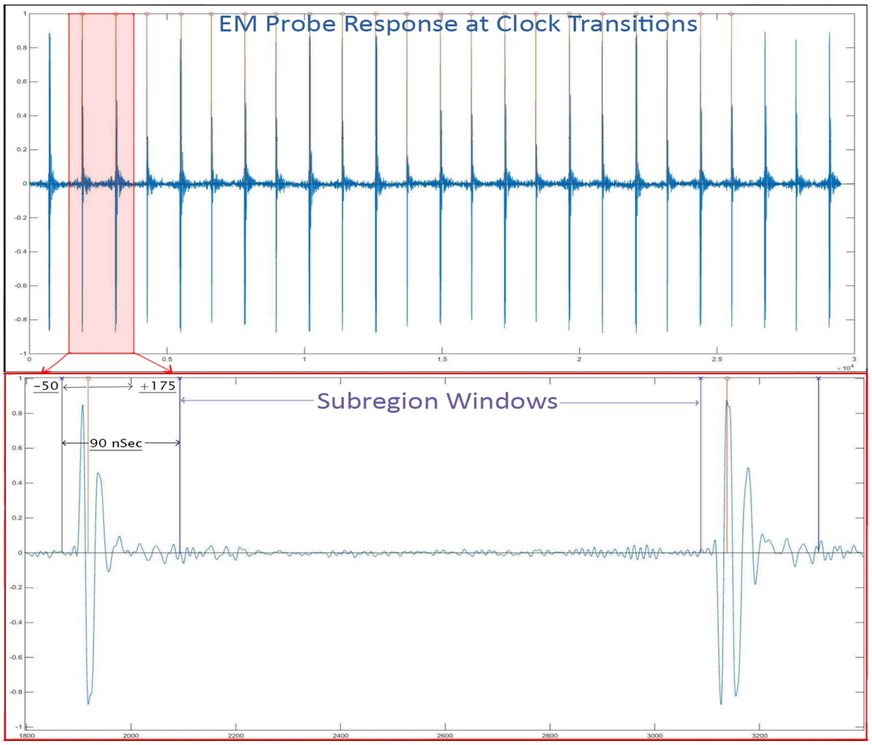


Figure 3.25. EM Probe Response and Subregion Windows.

With transistor wear-out impacting digital switching current, the Regions of Interest (ROI) for the signal is the response around the clock transitions where switching activity occurs. The rest of the URE signal between clock transitions is assumed to not contain data significantly impacted by wear-out induced changes. Keeping the

URE spikes around transitions and removing the URE response between transitions effectively increases the SNR of the wear-out related signal.

The sub-region window displayed in the right plot of Figure 3.25 includes 225 data values. At the 2.5 GSps oscilloscope sampling rate, this 225 samples equates to a 90 nano-second window. If the MSP430 operated at maximum speed and critical path transistors were sized for each transition to reach the required noise margin state within 80% of the next clock transition, 16 nano-seconds would be the required transition time. While the clock speed is reduced from max speed, the transistor sizing is fixed at time of manufacturing to allow operation at the maximum clock speed. Therefore the switching around each clock transition occurs in same time required for the max speed operation. The 225 sample window of 90 nano-seconds encompasses the transition time set by the MSP430 transistor sizing and critical path limitations. This 225 data point window therefore contains the signal related to transitions and wear-out alterations.

The window subregions also negate the effect of clock jitter present in the MSP430 master clock [62]. The observed clock frequency variability did not correlate with oven aging time and the centering of the 225 data point window on clock transitions eliminate this concern. The fingerprints defined with the 20 uniform subregions, did not removed the effects of clock jitter and the latter sub-regions could have up a 10 clock cycle offset.

3.2 Age Estimation

The methods used for *Age Estimation* are discussed before the other goals, because the attempts to improve performance also apply to the other goals. The purpose of *Age Estimation* was to determine if exiting RF-DNA techniques can be used to identify the cumulative run time of a device with unknown operational time. *Age Esti-*

mation was first attempted with the 20 uniform subregion single-location fingerprints. Consistent results were not achieved and attempts to reconcile lack of performance led to the multi-location transition-centric fingerprints mentioned in Section 3.1.6 and 3.1.7. The discussion explaining the changes in methodology and resulting multi-device fingerprints requires presentation of some results. Therefore, this section will present results used to refine the methodology.

3.2.1 *Age Estimation* - RF-DNA Training & Use

The application construct trained the MDA/ML classifier with three different oven ages (Age-0, Age-3, Age-7) that equate to an un-age device, a middle aged device and the max use device. Using a projection matrix based on training for the three ages indicated all other ages are projected into the hyperplane. The Euclidean distance of all projected fingerprints back to the Age-0 class are then plotted as a regression line. A device of unknown age can be projected down to the hyperplane, the Euclidean distance to Age-0 determined, and using the regression line the operational use time can be estimated.

3.2.2 *Age Estimation* - Results Format

Figure 3.26 shows the euclidean distance concept for the simulated results of Section 2.4.3 using the V_T shift employed in SPICE. This result was promising but when applied to actual MSP430 UREs, no combination of candidate locations nor devices resulted in a monotonic regression line.

Figure 3.27 displays a typical regression for actual URE emissions from a single location. *Age estimation* using such a regression was impossible because the possible age for the unknown device spanned the entire range of possible values.

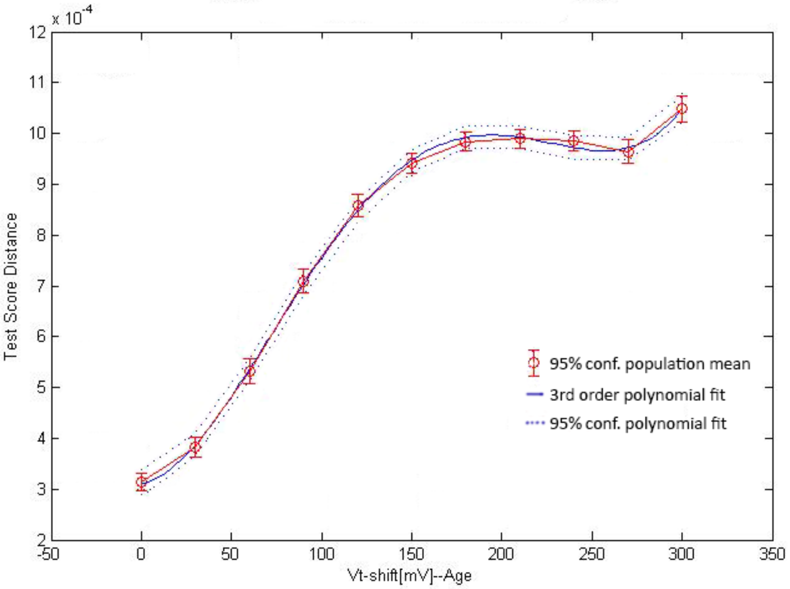


Figure 3.26. SPICE Simulated Age Estimation Regression Fit. Euclidean distance of all testing fingerprints to Age-0 training mean.

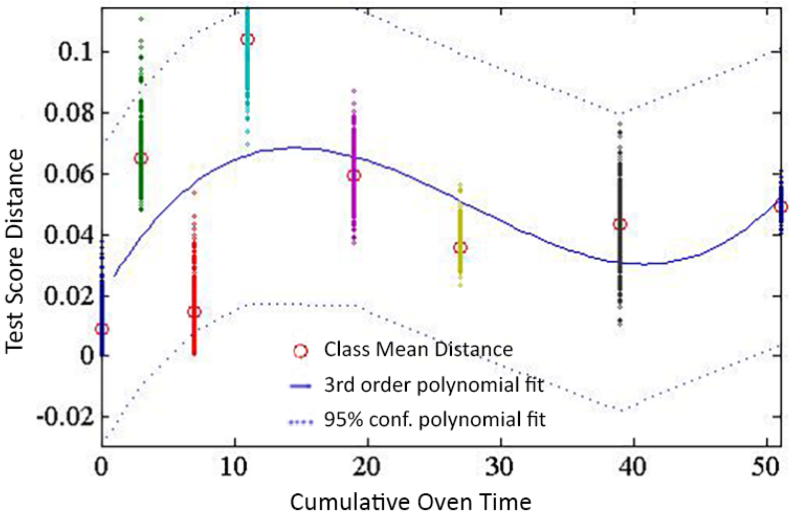


Figure 3.27. Experimental Age Estimation Regression Fit. Euclidean distance of all testing fingerprints to Age-0 training mean.

3.2.3 *Age Estimation* - Attempts to Improve Performance

Attempting to correct the unsuccessful age estimation led to the multi-location transition-centric fingerprints designed to reduce the repositioning impacts displayed in Figure 3.28. The three repositioning events impart distance changes on the order of distance changes stemming from the oven aging increments. As a result the Euclidean distance measure used to form the regression could not track device age.

Prior to developing multi-location fingerprints, GRLVQI was used in an attempt to identify common, performance improving, features across multiple single-location fingerprints. If common features for all training events were identifiable, the non-common features could be removed to improve the *age estimation* performance of the fingerprints. Removing the non-common features may reduce the reposition induced spread. Some common features were identifiable using GRLVQI but the resulting fingerprints did not satisfactorily address the non-monotonic age separation displayed in Figure 3.27.

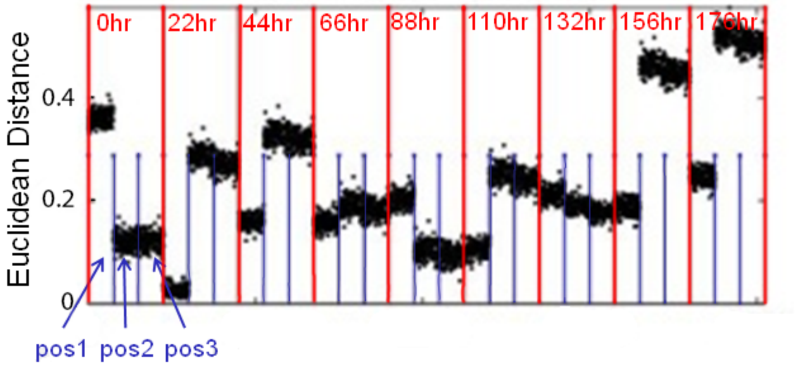


Figure 3.28. Euclidean distance of all Age-1 fingerprints to all Age cluster means. Blue lines delineate repositioning. Red lines delineate change in the age cluster mean reference

Despite efforts to reduce the reposition spread, the MDA/ML classifier was still unable to produce a monotonic regression for age estimation. The spread of the multi-location transition-centric fingerprints can be seen in the hyperplane projections of Figure 3.29. Using Euclidean distance to class Age-0 still results in a non-monotonic curve and the impact of repositioning is still observable as seen in the separation of the Cyan-Magenta-Yellow (CMY) clusters. The Red-Green-Blue (RGB) clusters show that MDA/ML training limits the reposition spread for the training-age fingerprints but the spread due to repositioning persists for the non-training-age fingerprints.

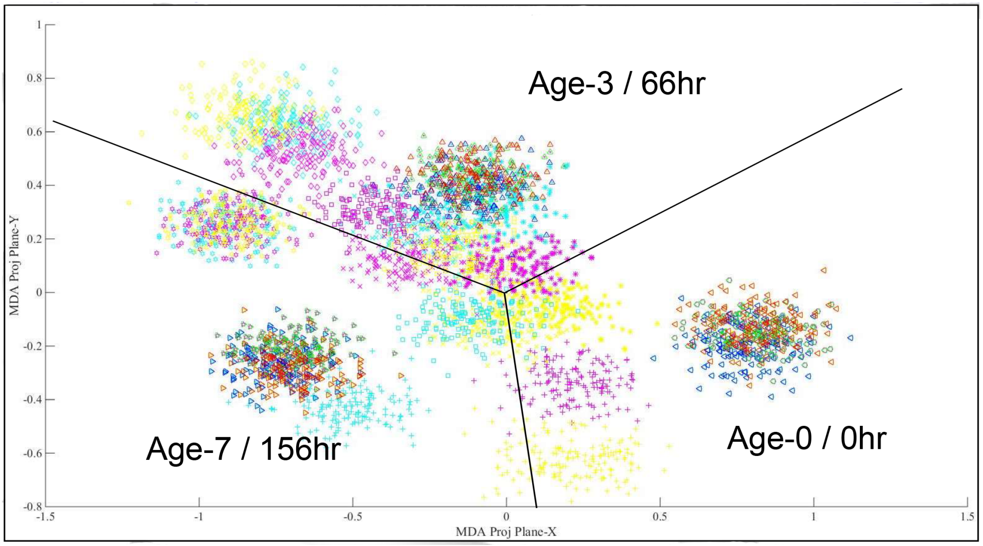


Figure 3.29. Multi-location Fingerprint Separation for Device C2. Triangles indicate training fingerprints. Non-triangle indicate testing fingerprints. RGB colors indicate the three training fingerprint repositions. CMY colors indicate the three testing fingerprint reposition.

3.3 Device Discrimination

Device Discrimination seeks to document wear-out impacts to the existing device discrimination construct of previous URE RF-DNA efforts [14, 15, 12, 11, 54, 64, 65]. As devices are in continual operation how long does an RF-DNA model remain applicable? Can the device discrimination application train on devices at one age and apply the training to all other ages? If age does impact features used to discriminate devices, classification performance will be a function of device age.

3.3.1 *Device Discrimination* - RF-DNA Training & Use

Like the *Age Estimation* efforts, *device discrimination* was not consistent across single-location fingerprints. Therefore multi-location transition-centric fingerprints where also used for device discrimination. As a reminder these fingerprints include the following features:

1. *Locations*: 9 central locations - 7, 8, 9, 12, 13, 14, 17, 18, 19
2. *Signal Attributes*: Instantaneous Amplitude only
3. *Moments*: Variance, Skewness, Kurtosis
4. *Subregions*: 16 windows with 225 data points at clock transitions
5. *Number of Features*: 432

With multi-location fingerprints, location was no longer a design variable in possible MDA/ML training, since the nine central locations were already in the fingerprints. The variables available to define different classes in the *Device Discrimination* effort were now only the device class and how many classes to use. If only two class problems are entertained, there are a possible 36 different device combinations. Three class problems were also explored with a 84 possible device separation combinations. Only the devices in the A-B-C group and of this group only the aged devices (1-3) were used, leaving a total of nine possible devices (A1, A2, A3, B1, B2, B3, C1, C2, C3). In addition, the order of device paring was not considered important; the paring of A1:A2:A3 was the same as A3:A2:A1.

The MDA/ML classifier was trained to separate multiple devices at one of the three training ages (Age-0, Age-3, Age-7). The resulting RF-DNA discrimination model was then applied to fingerprints for all ages and the classifier selected the device class for all the ages. If age wear-out impacts classification accuracy the correct determination for aged fingerprints should drop as the red dashed line shown in Figure 3.30 when the MDA/ML classifier is trained on Age-0 fingerprints. The use fingerprints at Age-0 should have each device identified correctly and there should

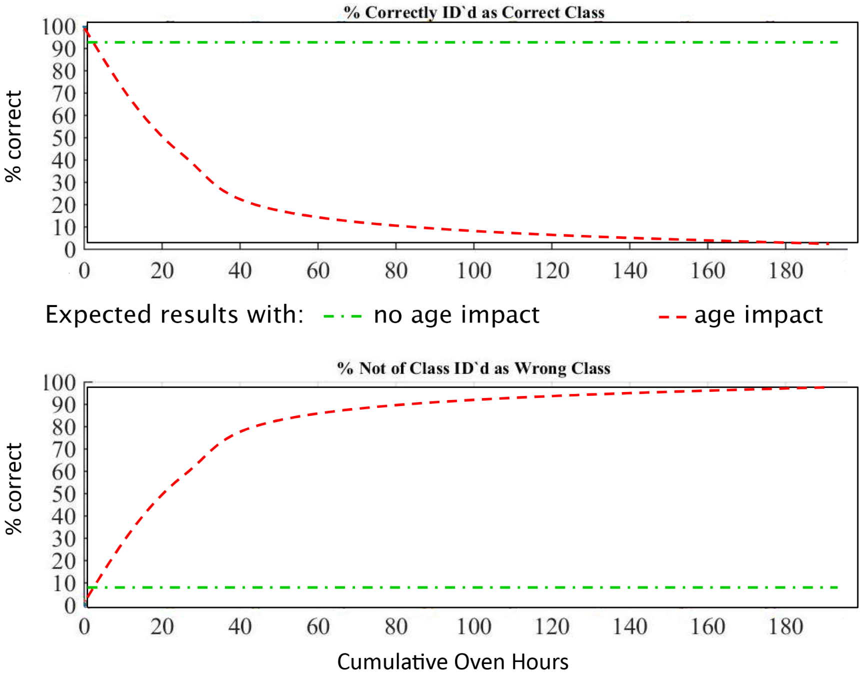


Figure 3.30. Possible Device Discrimination Performance with Aged Fingerprints.

be limited instances of false identification at Age-0. At higher ages, the correct identification and false identifications should degrade. If wear-out does not impact device discrimination the performance should be consistent across the device age categories.

3.3.2 *Device Discrimination* - Results Format

The results of Figure 3.31 are for a single combination (B1:B3) of the possible 36 (2-Class) device pairings. In this single discrimination of B1:B3 the higher age fingerprints do not perform accurately when using MDA/ML model developed for Age-0. This implies a single training age becomes less applicable as a device remains in operation.

Since this study seeks to determine if wear-out consistently impacts discrimination, the MDA/ML classifier was applied to all possible device discrimination parings. The aggregate results for all device combinations is then recorded for each of the three training ages. Age-0 training will have 36, or 84 for 3-Class, total discrimination tests and one total response result. Age-3 and Age-7 training will also have 36, or 84, individual tests and one aggregate response for each age. To determine if wear-out impacts device discrimination, each of the aggregate responses for each of the three training ages are compared.

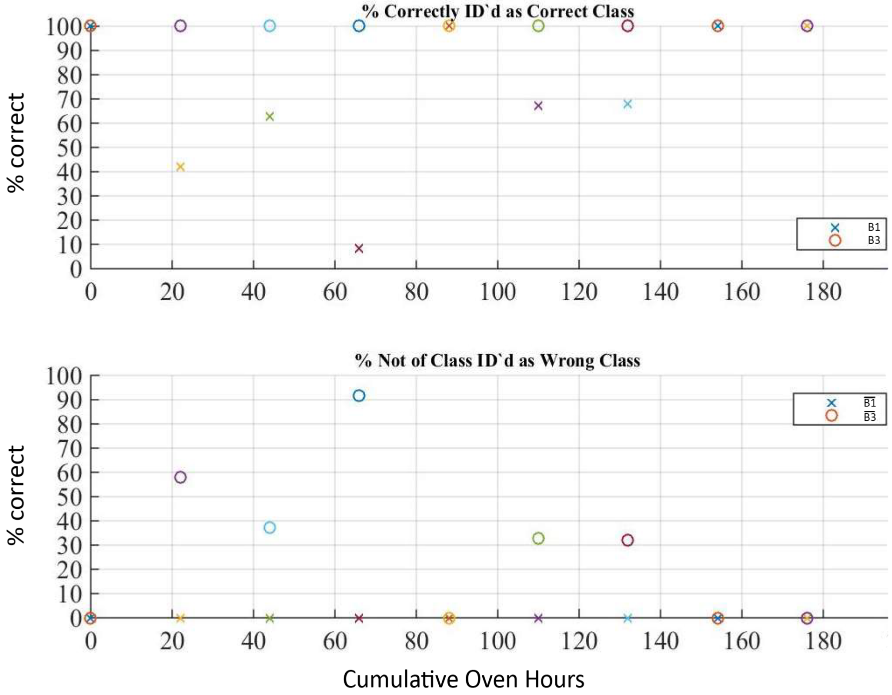


Figure 3.31. B1 vs. B3 MDA Classification Accuracy with Age-0 Training. Top: correct classification. Bottom: false classification, calling B3 as B1 or B1 as B3. X-axis: cumulative oven age time. Y-axis: percentage correct for all fingerprints.

The aggregate of all Age-0 responses produces distributions as shown in Figure 3.32. Each training age (Age-0, Age-3, Age-7) will have a similar plot. This quad chart documents the correct identification rate for all 2-class combinations in the top-left and bottom right subplot as labeled in the subplot title. The top-right and bottom-left subplots show the false classification results as labeled in the subplot title. These plots are histogram distributions of all possible 2-class problem results. The histogram bins are 1% wide and centered at 1/2% values resulting in 100 bins, one for each % value.

Ideal response in the top-left and lower-right plots would be a single spike at 100%. A single spike would indicate all of the 2-Class parings, with 450 individual fingerprint tests per age for each device, never missed a correct identification. It is also possible to have 36 individual spikes all at 2.78%, one for every 2-Class combination. Ideal response for the top-right and bottom-left subplots would be a single spike at 0%. A spike at 0% signifies a collection of perfect classification runs with each run never falsely identifying a device.

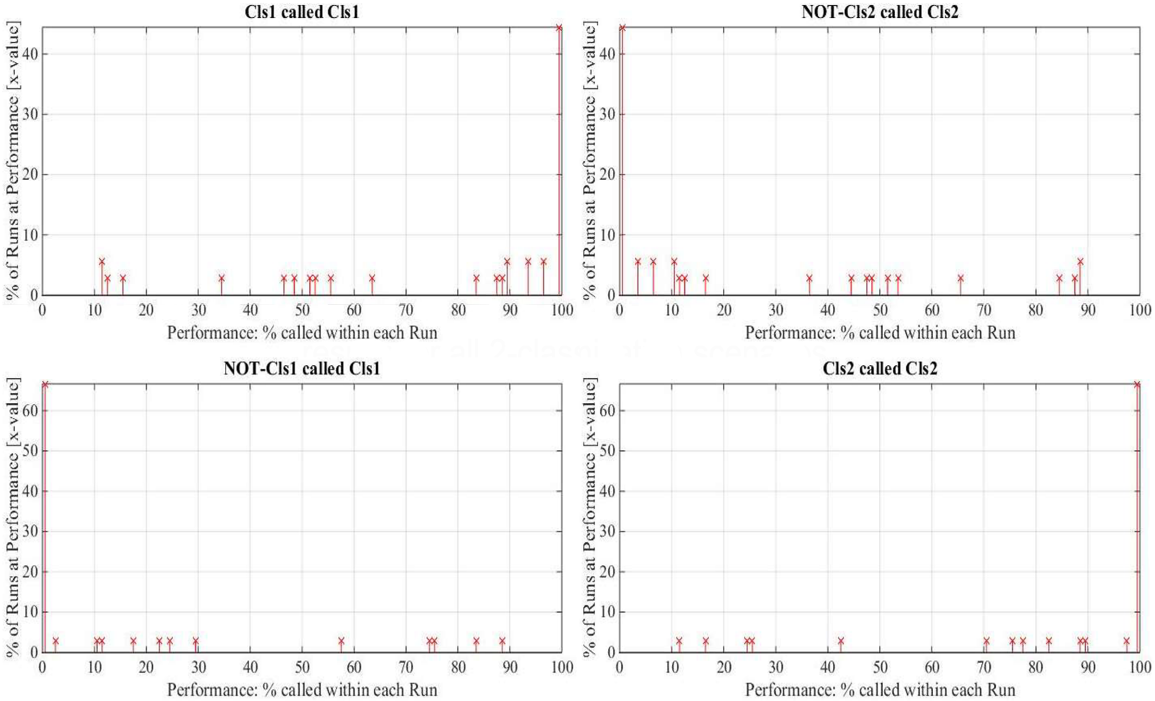


Figure 3.32. Discrimination Accuracy for all 2-Class Pairings. Includes 36 Runs (9 choose 2, order not important) with all nine Ages. Top-left and Bottom-right document true identification rates. Top-right and Bottom-left document false identification rates.

Since the aggregate responses can have varying level of performance the comparisons between the three training ages is done by producing a Cumulative Distribution Function (CDF) for each aggregate response. The three CDFs can then be plotted on the same scale for comparison. Performance is indicated by the area under the CDF curves. Ideal response for correct identifications would have no area under the CDF curve from the single spike at 100%. Ideal response for correct False Identification would have the max area under the CDF curve due to a single spike at 0%. The CDF plots for the 2-Class and 3-Class scenarios are presented in Section 4.1. These combined CDF plots show the aggregate impact of wear-out on device discrimination.

The previous result methods can not isolate the impact of induced wear-out (oven age increments) from repositions. Observing the impact of repositioning requires plotting results on the MDA/ML hyperplane and thus can only be done for a single run at a time since each run conducts is own MDA/ML training creating a new hyperplane. To examine all repositioning impacts would require 108 plots (36 runs times 3 training ages) in the 2-class case and 252 plots (84 runs times 3 training ages). Instead, Section 4.1.3 displays one case of repositioning impact which implies repositioning does have an impact but that the dominate change in classification performance is due to wear-out.

3.4 Age Discrimination: Aged vs. Un-aged

Device Discrimination only utilized the incrementally aged devices from the A-B-C group. However, when the *Device Discrimination* techniques were applied to 2-Class cases with one device from the aged A-B-C group and the other from the non-oven aged device list (A4, B4, C4), the results indicated a binary classifications approach may be beneficial. The original goal of *age estimation* attempted to determine how long an unknown device was in operation. This binary age estimation, called *Age Discrimination*, is a 2-class simplification of *age estimation* and seeks to determine if an unknown device is un-aged (new) or aged (used) using RF-DNA features and the MDA/ML classification method. Success with *age discrimination* provides a means to identify recycled devices.

The ROC curve in Figure 3.33 indicates the wear-out induced movement of C4 within the MDA hyperplane is not as severe as the wear-out induced movement of

C1. The distributions of the C4 fingerprint at all ages stays closer aligned to the distributions of the Age-0 C4 training fingerprints. Whereas, the distribution of C1 fingerprints at all ages are always farther removed from the distribution of Age-0 C1 training fingerprints. The one exception for C1 comes with C1 use fingerprints at Age-0 compared to the C1 Age-0 training fingerprints. This single exception is expected because these distributions should be almost equivalent since they are the same event, one 900 burst collection set vs. the other 900 in the doubled up signal collection, see Section 3.1.5. Other combinations of the A-B-C oven aged devices compared against A4, B4, C4 produced similar ROC curves.

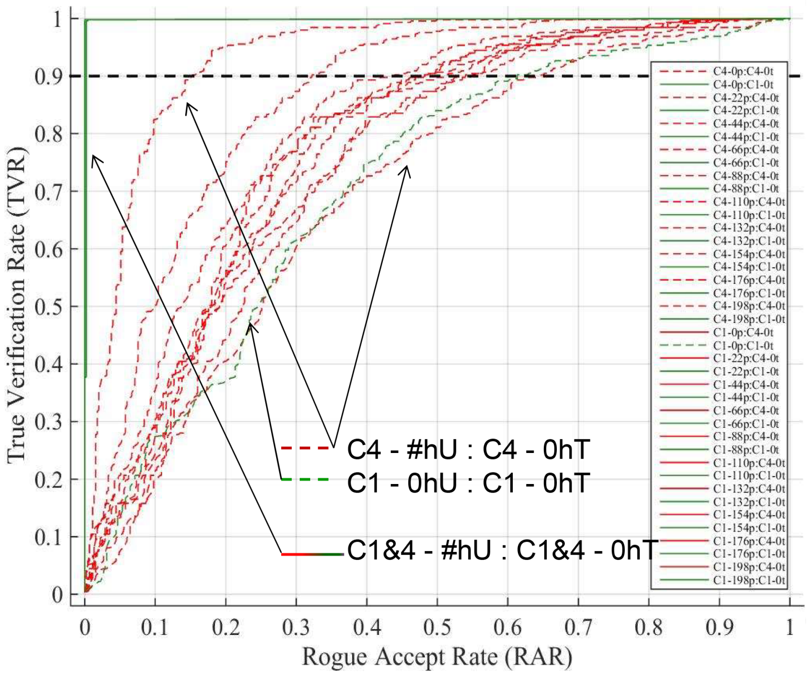


Figure 3.33. ROC distributions for all ages of C1 & C4 against C1 & C4 at Age-0. #hU indicates testing results for all fingerprint ages; each trace corresponds to a single age. Testing fingerprints are compared to C1 or C4 Age-0 training fingerprints.

3.4.1 *Age Discrimination* - RF-DNA Training & Use

Age Discrimination uses the same multi-location transition-centric fingerprints as the *Device Discrimination* effort, but class definitions used for MDA/ML training are re-defined. Instead of training each device as a separate class, the classes are defined as all fingerprints that are un-aged (Age-0 training fingerprints - Class 1) or aged (combination of Age-3 and Age-7 fingerprints - Class 2). The combining of Age-3 and Age-7 was done by using half of the 900 fingerprints from Age-3 combined with half of the 900 fingerprints from Age-7. Additionally the classes incorporated multiple devices and the devices did not have to remain the same in both Class-1 and Class-2.

Each class can use between one and three different devices. In all instances, three device slots are used for Class-1 and Class-2 but these slots can be filled with the same device three times or three different devices can be used. The slots in Class-1 do not have to be the same used for the slots in Class-2. Using different devices allows device variability as a means to force the MDA/ML classifier to find the fingerprints features stemming from the wear-out variations rather than device-to-device variability. For example Class-1 (un-aged) may be trained with all the Age-0 fingerprints from devices A1, B2, and C3. Class-2 may be trained with fingerprints from A2, B3, C2.

3.4.2 *Age Discrimination* - Results Format

Using the MDA/ML model developed with three devices in each class allows results testing with up to nine different device. For example the single run discrimination results shown in Figure 3.34 use the classes as defined in the previous paragraph but test the age vs. un-age classification using Devices A3, B1, C1. None of the nine device slots used a repeated device. This case tests the ability to determine aged vs. un-age devices without repeating any devices in both the two training classes nor use events. There is no way, the MDA/ML classifier could have trained on features due to device variation since the use devices were never presented for training. In this case the Age-0 fingerprints for A3, B1, and C1 were correctly identified as un-aged at a rate of 90%. The aged fingerprints (all fingerprints collected after oven aging) were correctly identified as Aged at a rate better than or equal to 80% depending on the specific age examined. This plot is produced in the same manner as the single run Device Classification result of Figure 3.31. The difference between *Device Discrimination* and *Age Discrimination* comes for the interpretation of the results since the classes are no longer different devices but defined by the vertical line between Age-0 (Un-aged) and Age-1 (Aged: all ages greater than Age-0) in the plot. This Figure 3.34 result follows the idea of training on a subset of devices and then using the model in the future to test if new products are previously used items.

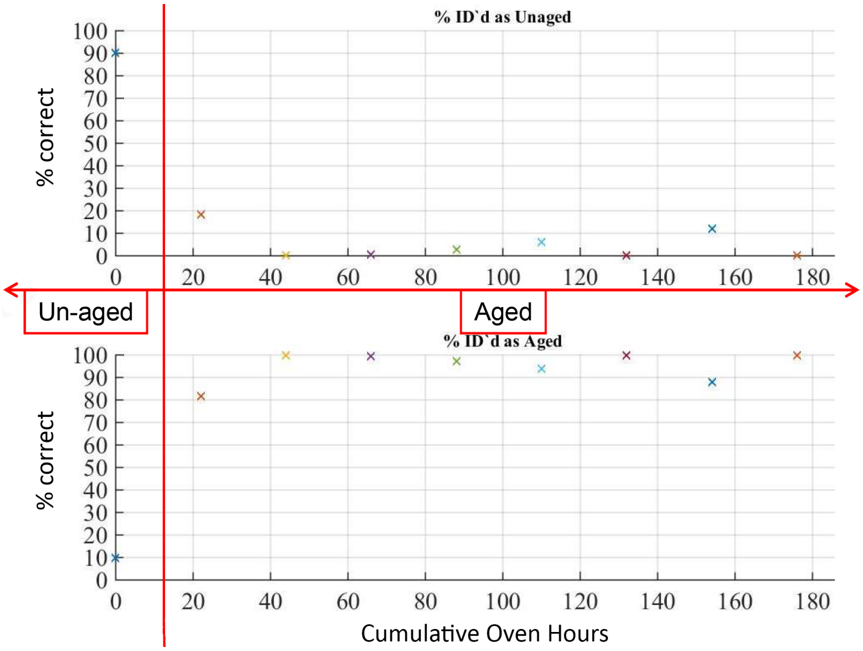


Figure 3.34. Aged vs. Un-aged Accuracy. Class-1: A1-B2-C3 Age-0 Fingerprints, Class-2: A2, B3, C3 Age-3 & Age-7 Fingerprints. Use Fingerprints from A3, B1, C1. X-axis: cumulative oven age time. Y-axis: percentage correct for all test/use fingerprints.

For determining the consistency of this *Age Discrimination* technique, the single run results as shown in Figure 3.34 are accumulated in aggregate for all possible device combinations just as was done for the *Device Discrimination* effort. Since the two classes and use/testing set are defined by nine different device slots, the number of runs can be defined in multiple ways.

In the *Device Discrimination* tests, the three different training ages were used to define three different aggregate results. For *Age Discrimination*, three aggregate results are again used but the variability of selecting devices in the nine device slots was used to define a Best Case, Worst Case and Random Case aggregate result.

The Best Case forces all nine device slots to use the same devices. The three devices used to define Class-1 (Age-0/Un-aged) are also used to define Class-2 (Aged) as well as fill the three device slots in the Use/Testing set. This scenarios test multi-device and single-device results since the device slots can be the same Device; A1-A1,A1 is a possible combination. Forcing Class-1, Class-2, and Use Sets to use the same devices creates 729 possible combinations requiring 729 individual MDA/ML runs.

Figure 3.35 shows the aggregate response for the Best Case/Same Device scenario. The Un-Aged label only includes Age-0 fingerprints. The Aged label averages the classification performance for all the oven ages – results to the right of the vertical dividing line in Figure 3.34. Because the Aged category includes multiple age fingerprint results, there is more opportunity for reduced performance. In the top subplots (Un-aged called...) there are only 729 possible results, one from each MDA/ML run. In the bottom subplots (Aged called...) there are 5832 possible results, 729 runs times eight different ages.

The Worst Case training scenario forces the Use/Testing set devices to be devices not used for training. Like the Best Case scenario, Class-1 and Class-2 are defined with the same three devices. However, the three device in the Use set are randomly selected from the six other devices not used for training. The scenario also required 729 individual MDA/ML runs.

The Random Case allows all nine device slots to be randomly selected from nine devices in the A-B-C / 1-3 set. This random selection is done without replacement for Class-1, Class-2 and Test/Use Set. Class-1 can be any of 504 combinations. Class-

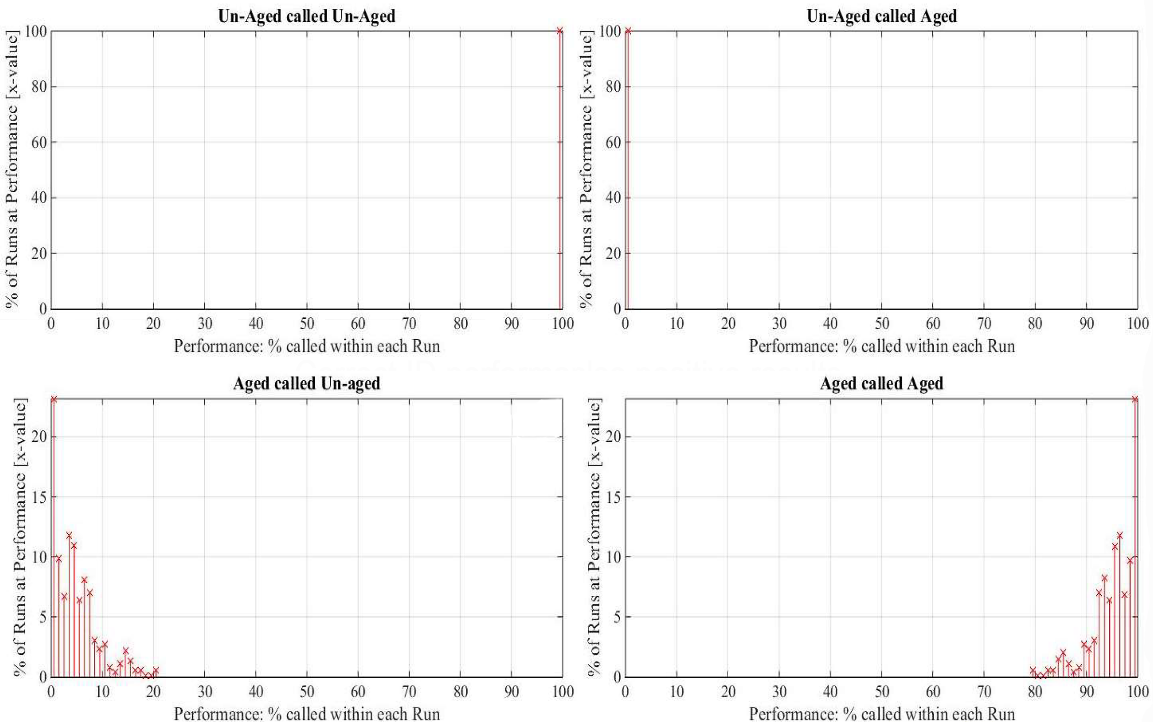


Figure 3.35. Age Discriminations for Best Case/Same Devices. Includes 729 Runs (9 permute 3) with all nine Ages. Top-left and Bottom-right present true identification rates. Top-right and Bottom-left present false identification rates.

2 can also be any of 504 combinations. The three devices in Class-1 can be the same as Class-2 but this is not forced nor prevented. This scenario then has 254,016 possible training combinations. Unlike the previous case that exhausts all training combinations, the Random Case only accomplished 5000 randomly selected runs out of the 254,016 possible training combinations.

The aggregate results of the three test scenarios are compared through their CDFs similar to the technique used in *Device Discrimination*. In *Device Discrimination*, the comparisons of CDFs was used to demonstrate accuracy degradations due to wear-out phenomenon. In *Age Discrimination*, the CDF comparisons are used to show the range of accuracy using best and worst case training and testing scenarios.

The aggregate performance and CDF procedures above are also applied to the control devices A4, B4, C4, D1, D2, E1, and E2. The results using the control devices in the Use/Testing Set displays the ability to determine new versus used devices that were not incrementally aged.

Discrimination based on device differences should be negligible in *Age Discrimination* due to class definition by age and training with multiple devices. However, the impact of repositioning may still be present. As was the case in *Device Discrimination*, the age impact versus reposition impact can not be decoupled. The Results Section 4.3.2 provides a few MDA/ML hyperplane projections giving insight to the relative influence of device repositioning.

IV. Results

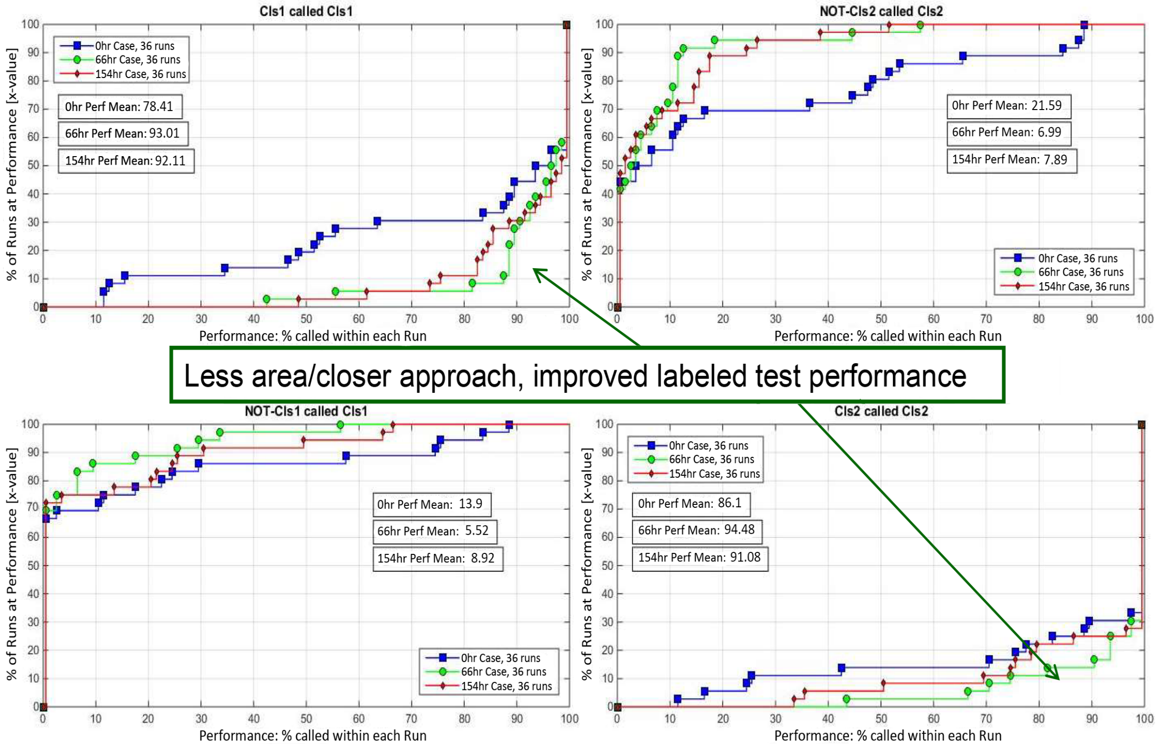
This chapter presents the experimental results for the three wear-out research goals: *Device Discrimination*, *Age Estimation* and *Age Discrimination*. Section 4.2 – *Age Estimation* does not include any additional plots or data than what is presented in the Section 3.2. The results discussed in *Age Estimation* methodology demonstrate the inability to achieve the age estimation goals using the devices, wear-out age acceleration, and RF-DNA techniques of this research. The results for the other goals, *Device Discrimination* and *Age Discrimination*, both use CDFs that aggregate all iterative MDA/ML results from multiple classification tests. The CDF plots appear similar for both goals, but different training methods described in Sections 3.3.1 and 3.4.1 alter the interpretation of the CDFs. Additionally, the impact of repositioning is also addressed for both *Device Discrimination* and *Age Discrimination*.

4.1 Device Discrimination

IC wear-out can impart observable alterations when using the RF-DNA discrimination techniques with Unintentional Radio Emissions (URE). Initial training at Age-0 is less accurate when used for devices running over a month of operation. Training at subsequent ages (Age-3 and Age-7) provides increased accuracy when applied to all ages for both the 2-Class Discrimination and 3-Class Discrimination cases.

4.1.1 Two Class Results

Figure 4.36 is the culmination of the 2-Class device discrimination methodology. Top-left and bottom-right plots show correct identification results as labeled in each subplot title. Ideal response is a spike at 100% with no area under the CDF curve. Top-right and bottom-left plots show the false identification results as labeled in each subplot title. Ideal response is a single step at 0% with all plot area enveloped by the CDF. Each training age is signified as follows: Age-0 training with blue-squares; Age-3 training with green-circles, Age-7 training with red-diamonds.



Less area/closer approach, improved labeled test performance

Figure 4.36. Device Discrimination CDF for all 2-Class Pairings. Includes 36 Runs (9 choose 2, order not important) with all nine Ages. Top-left & Bottom-right: true ID rates. Top-right & Bottom-left: false ID rates.

The CDFs for experiments using the higher age training models indicate improved sustained performance. Each CDF is for all 36 possible 2-Class discrimination tests. Both the correct identification rates and false classification results improve. True identification results move closer to 100%. False rates move closer to the 0% ideal. Summary of average classification performance is listed in Table 4.4.

4.1.2 Three Class Results

Figure 4.37 is the culmination of the 3-Class device discrimination methodology. Top plots show correct identification results as labeled in each subplot title. Ideal

Table 4.4. 2-Class Average Performance for the three Training Ages.

Average Identification Rate		
	Class-1 called Class-1	NOT Class-2 called Class-2
Age-0 Train	78.41	21.59
Age-3 Train	93.01	6.99
Age-7 Train	92.11	7.89
	NOT Class-1 called Class-1	Class-2 called Class-2
Age-0 Train	13.90	86.10
Age-3 Train	5.52	94.48
Age-7 Train	8.92	91.08

response is a spike at 100% with no area under the CDF. Bottom plots show the false identification results as labeled in each subplot title. Ideal response is a jump at 0% with all plot area enveloped by the CDF. Each training age is signified as follows: Age-0 training with blue-squares; Age-3 training with green-circles, Age-7 training with red-diamonds.

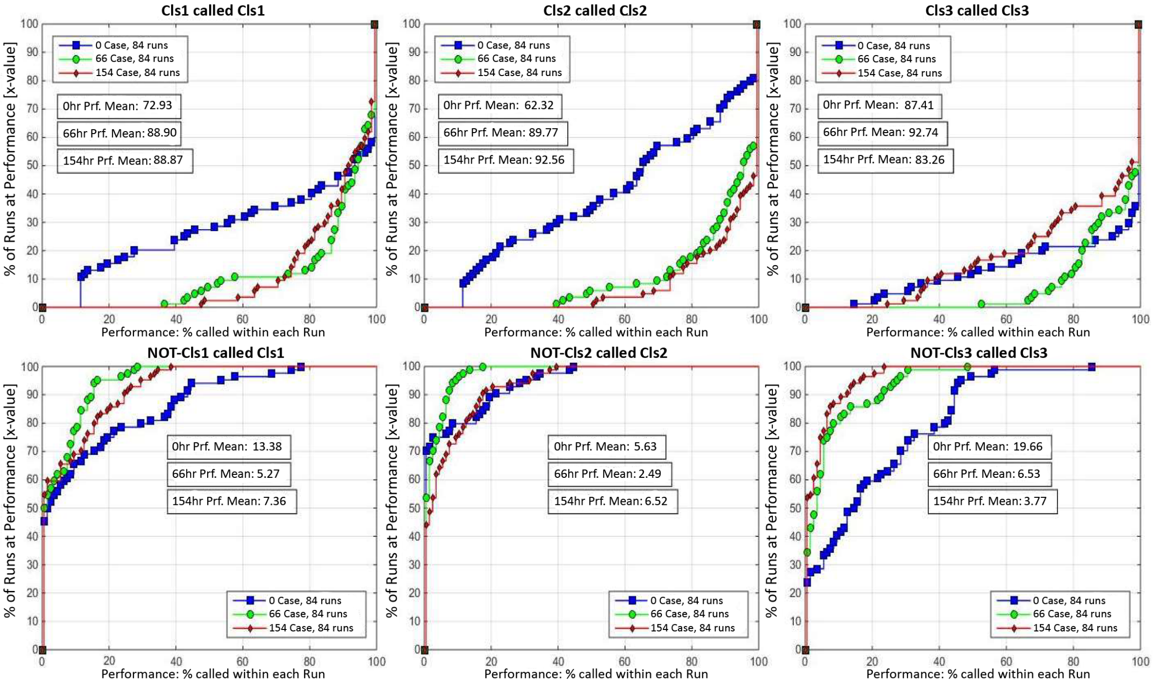
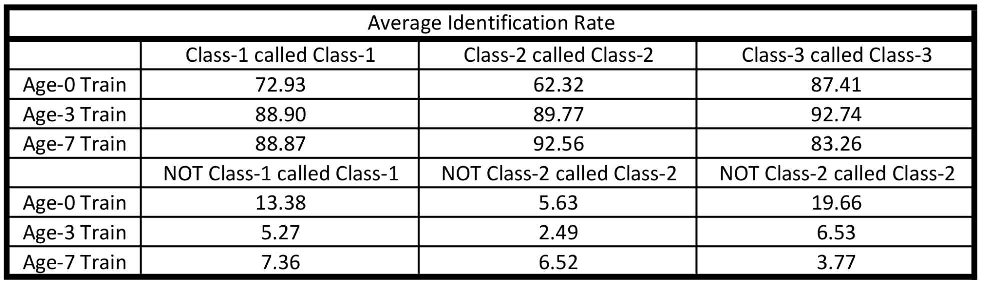


Figure 4.37. Device Discrimination CDF for all 3-Class Pairings. Includes 84 Runs (9 choose 3, order not important) with all nine Ages. Top: true ID rates. Bottom: false ID rates.

The CDFs for experiments using the higher age training models indicate improved sustained performance when compared to the results of the Age-0 training models. Each CDF is for all 84 possible 3-Class discrimination tests. Both the correct identification rates and false classification results improve, except for the Age-7 (154-hr) results for Class-2 and Class-3. In general the true identification results move closer to 100% and the false identification rates move closer to the 0% ideal. With the two exceptions, both the true identification and false identification rates do not simultaneously improve. The true classification accuracy for Class-3 using Age-7 training does not improve over Age-0 training, but the false identification rate does improve. The Class-2 results are the opposite with the false identification rate not improving but the true identification rate showing greater performance.

Summary of average classification performance is listed in Table 4.5. In the case of Class-3 results, the true identification performance drops from an average of 87.41% with Age-0 training down to 83.26% with Age-7 training. However, the false identification rate related to Class-3 improves dramatically improves from 19.56% with Age-0 training down to 3.66% with Age-7. The Class-2 exception is also observed in the average performance with the false identification rate slightly increasing for Age-7 training, while the true identification rate improves with Age-7. The Class-1 average results show simultaneous improvements in both the true and false identification averages.

Table 4.5. 3-Class Average Performance for the three Training Ages.



Average Identification Rate			
	Class-1 called Class-1	Class-2 called Class-2	Class-3 called Class-3
Age-0 Train	72.93	62.32	87.41
Age-3 Train	88.90	89.77	92.74
Age-7 Train	88.87	92.56	83.26
	NOT Class-1 called Class-1	NOT Class-2 called Class-2	NOT Class-2 called Class-2
Age-0 Train	13.38	5.63	19.66
Age-3 Train	5.27	2.49	6.53
Age-7 Train	7.36	6.52	3.77

4.1.3 Repositioning Impact

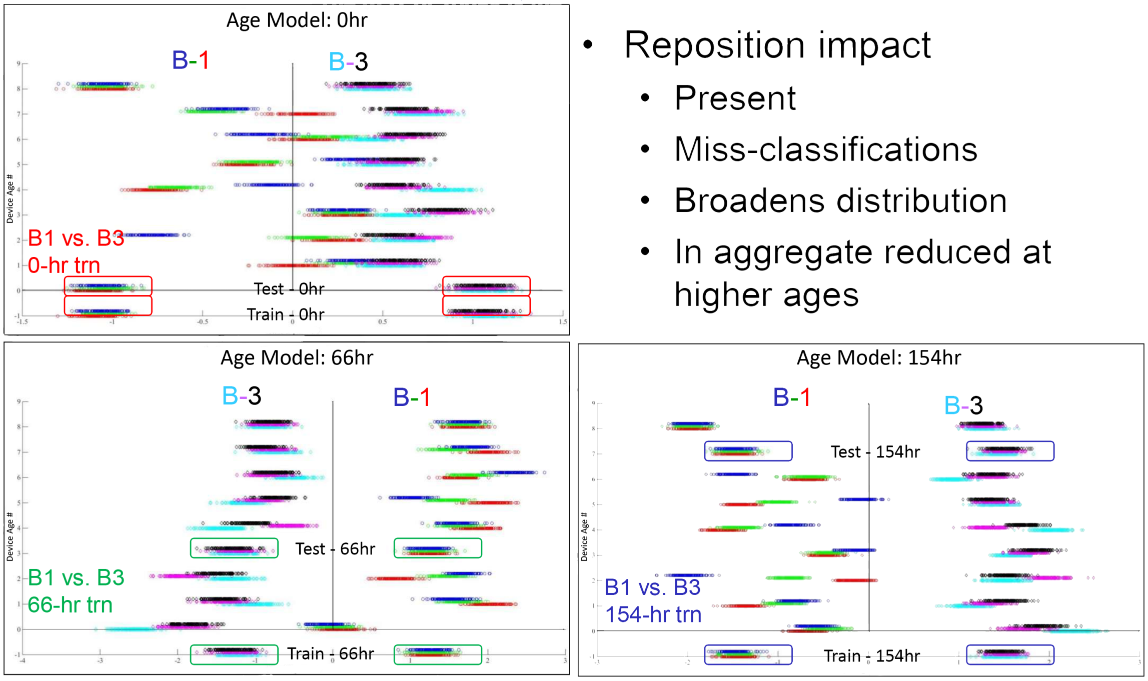
Figure 4.38 demonstrates representative repositioning impacts to the *Device Discrimination* results. The lowest clusters are the projection of training fingerprints. Use fingerprints with ages from Age-0 to Age-8 are along the Y-axis. The X-axis is the projected position on one dimensional MDA/ML hyperplane. Red-Green-Blue colors show each of three repositioning events for B1 fingerprints. Cyan-Magenta-Black colors show each of three reposition events for B3 fingerprints.

At all training ages, repositioning results in some errors – projections incorrectly crossing the classification boundary. The errors are more prevalent in the Age-0 results with multiple different age clusters crossing the device classification boundary. In the Age-66 results only one cluster, B1 at Age-0, crosses the boundary. Age-154 results only have a few instances in the tails of some B1 clusters crossing the boundary. This single B1:B3 run would result in improved classification as the training age is changed from Age-0 to Age-3 and Age-7 just as is seen in the aggregate CDFs in Figure 4.36. Even with such reposition impact, wear-out is the dominant effect on device classification accuracy. Higher age training may reduce the impact of repositioning.

4.2 Age Estimation

Age Estimation was not successful using MDA/ML RF-DNA techniques with either single-location uniform subregion fingerprints nor with multi-location transition-centric subregions. Possible reasons for this outcome include:

1. Repositioning imparts variation that is on the same order as the variation due to incremental wear-out / oven aging. As explained with Figure 3.28 in Section 3.2.3.



- Reposition impact
  - Present
  - Miss-classifications
  - Broadens distribution
  - In aggregate reduced at higher ages

Figure 4.38. Device Discrimination Repositioning Impacts. Projection of all B1 and B3 fingerprints ages when trained at Age-0, Age-3, and Age-4.

2. MDA/ML class training separates classes equidistant from each other. For *Age Estimation*, the class separation needs to place higher-age events at increasing distance from the un-age class.

No additional plots are presented here than what exist in Methodology Section 3.2. Relevant plots justifying this outcome were used in the methodology sections when describing the additional efforts to obtain successful *Age Estimation*. The additional efforts, while not fruitful for *Age Estimation*, ultimately enabled success with *Device Discrimination* and *Age Discrimination*.

4.3 Age Discrimination: Aged vs. Un-aged

The following results indicate RF-DNA techniques may enable recycled part detection. Using MSP430 micro-controllers and oven accelerated aging with up to one month of operational run time, new vs. used devices were correctly identified with performance between 78.7 - 99.9% for three testing cases. Addressing repositioning errors may further improve this performance.

4.3.1 Accuracy Worst to Best Case

Figure 4.39 is the culmination of the age discrimination methodology. Top-left and bottom-right subplots show correct identification results as labeled in each subplot title. Ideal response is a step at 100% with no area under the CDF. Top-right and bottom-left subplots show the false identification results as labeled in each subplot title. Ideal response is a jump at 0% with all plot area enveloped by the CDF. Each Use/Test fingerprint set is signified as follows: Excluded Devices with blue-squares; Random Devices with green-circles: Same Devices with red-diamonds.

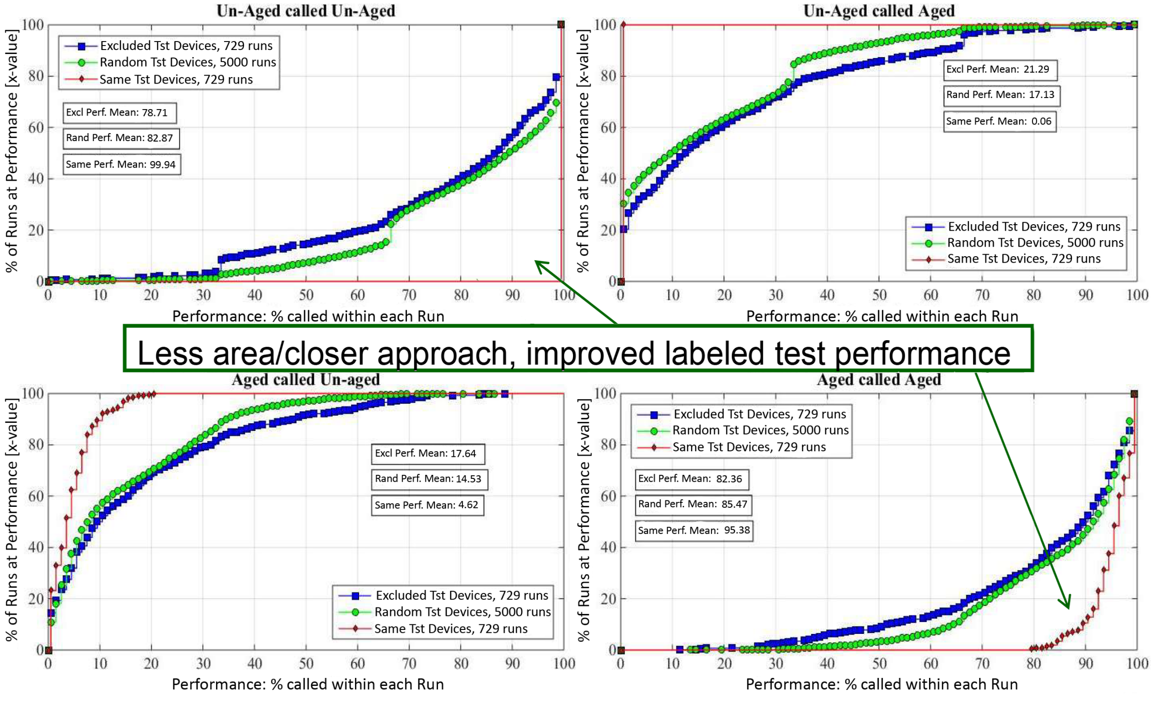
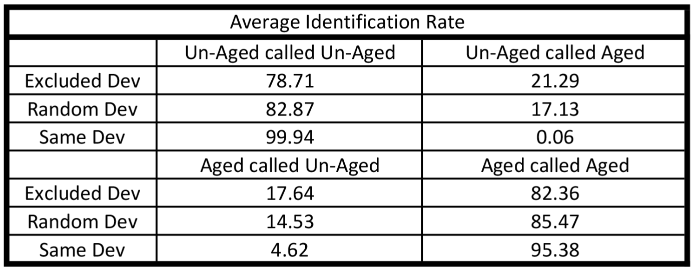


Figure 4.39. Un-age vs. Aged Discrimination CDF. Top-left & Bottom-right: true ID rates. Top-right & Bottom-left: false ID rates.

The average performance for each case is shown in Table 4.6. Even in the worst case, the correct identification as Un-Aged or Aged is 78% and 82% respectively and the false identification results are 21.29% or 17%. In the worst case scenario all four classification cases result in performance better than random 85% of the time.

Table 4.6. Un-aged vs. Aged Average Performance for the three Test scenarios: Excluded Use Devices, Random Use Devices, and Same Use Devices.

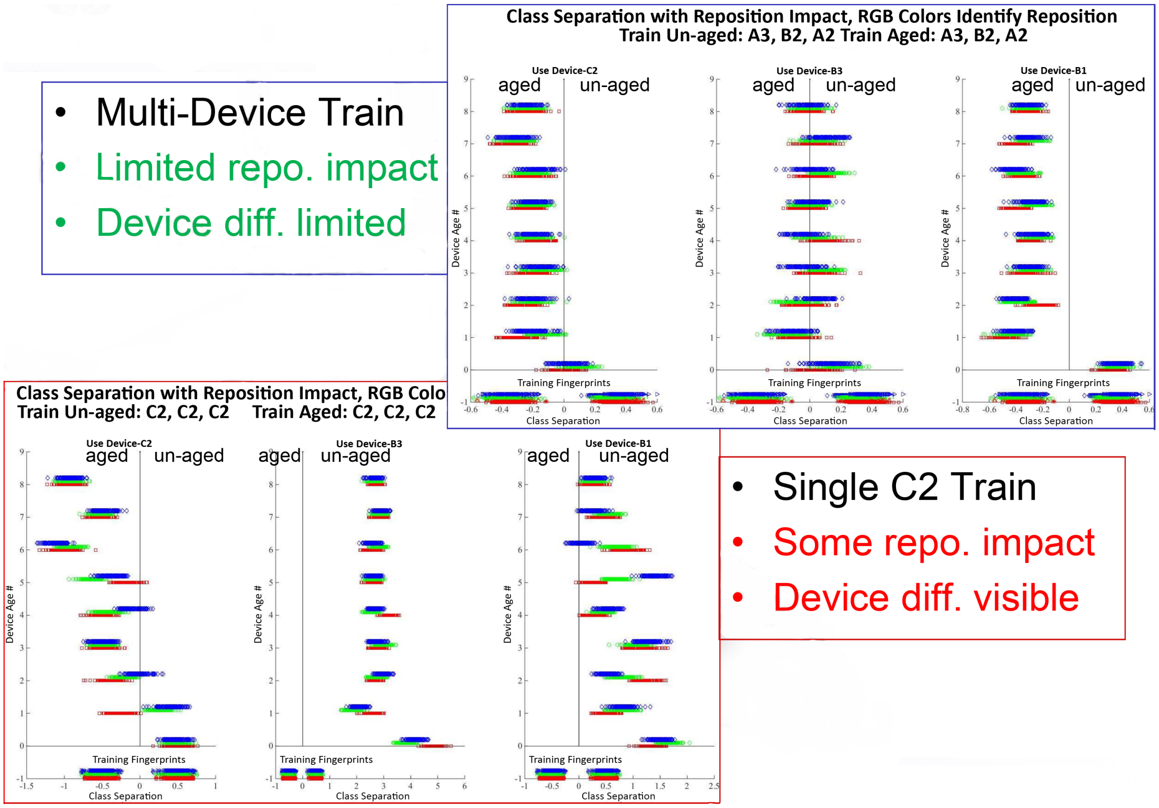


Average Identification Rate		
	Un-Aged called Un-Aged	Un-Aged called Aged
Excluded Dev	78.71	21.29
Random Dev	82.87	17.13
Same Dev	99.94	0.06
	Aged called Un-Aged	Aged called Aged
Excluded Dev	17.64	82.36
Random Dev	14.53	85.47
Same Dev	4.62	95.38

4.3.2 Repositioning Impact

Figure 4.40 demonstrates repositioning has less effect as compared to the results in *Device Discrimination*. Lowest clusters are the training results. Use Fingerprints with ages from Age-0 to Age-8 are along the Y-axis. The X-axis is the projected position on the one dimensional MDA/ML hyperplane.

The top plot using multi-device training (A3, B2, A2) and projection of device fingerprints not in the training set (C2, B3, B1), shows repositioning has almost no impact. All three reposition clusters are tightly bound to each other. The bottom plot trains on a single device (C2 is repeated in each of the three device slots for Class-1: Un-Aged and Class-2: Aged). The bottom projections are of the same devices used in the top plot with C2, B3, and B1. The results for C1, left column, and B1, right column, show some repositioning impact but most clusters stay on one side of the classification boundary. The B3 projection, center column, shows minimal repositioning impact but the entire column is far removed from the training class centers displaying a device dependency. These plots demonstrate repositioning impact, while still present, is not as severe as in the *Device Discrimination* efforts and device dependency is mitigated by training with multiple devices.



Class Separation with Reposition Impact, RGB Colors Identify Reposition
Train Un-aged: A3, B2, A2 Train Aged: A3, B2, A2

- Multi-Device Train
- Limited repo. impact
- Device diff. limited

Class Separation with Reposition Impact, RGB Colo
Train Un-aged: C2, C2, C2 Train Aged: C2, C2, C2

- Single C2 Train
- Some repo. impact
- Device diff. visible

Figure 4.40. Age Discrimination Repositioning Impacts. Top: multi-device training & test devices not in the training set. Bottom: single-device training & testing with same devices as the top plot.

4.3.3 Control Devices

The same CDF plot technique is applied to the control devices in the next three plots. The Use Devices in the first plot include A4, B4, C4. Devices D1 and D2 are used in the second. Finally, E1 and E2 are tested together in the last plot. All control devices behaved as expected except A4 and B4.

Oven Hold Out: A4, B4, C4

The Class-1 training set was modified to include Age-0 fingerprints for A4, B4, or C4 in one of the three device slots. Recall the two classes were defined using fingerprints from three devices in each class definition, see Section 3.4.1. The three device slots in the Class-2 definition were not modified and maintained the same devices defined by the 729 possible device combinations from the [A-B-C][1-3] set. If Class-1 (Age-0) did not include the Age-0 fingerprints from the control devices, results were inaccurate due to the device dependency phenomenon observed in the B3, center column, projection of Figure 4.40.

A4, B4, C4 were never oven aged and the expected results in Figure 4.41 should be a determination always calling all fingerprints as Un-aged. In the top-left plot all Age-0 fingerprints are correctly identified as Un-aged. Likewise, the top-right plot never calls Age-0 fingerprints Aged. In the bottom-right the labeled Aged fingerprints (Age-1, Age-2,....Age-8) should never be called Aged. A correct determination in this plot occurs by failing to obtain the labeled result, a CDF that starts at 0%. In the bottom-left subplot the fingerprints label as Aged (Age-1, Age-2, ...Age-8) are actually Un-aged and the expected response here is a CDF comprised of a step at 100%. Only C4 responds as expected in all subplots. A4 and B4 appear to have fingerprints that display aged characteristics despite never being oven aged.

A4 & B4 Errors

The plots in this section demonstrate A4 and B4 may have some wear-out type features despite never being oven aged. If this is the truly the case the *Age Discrimination* technique is sound and no errors were actually encountered.

Figure 4.42 plots A4, B4, and C4 fingerprints on the MDA/ML hyperplane for two of the 729 runs. The top projections train with Class-1 set to X4, A2, A3 and Class-2 set to A1, A2, A3. The bottom projections train with Class-1 set to X4, C1, C3 and Class-2 set to B1, C1, C3. The X4 indicates the first slot of three in Class-1 training is replaced with either A4, B4 or C4.

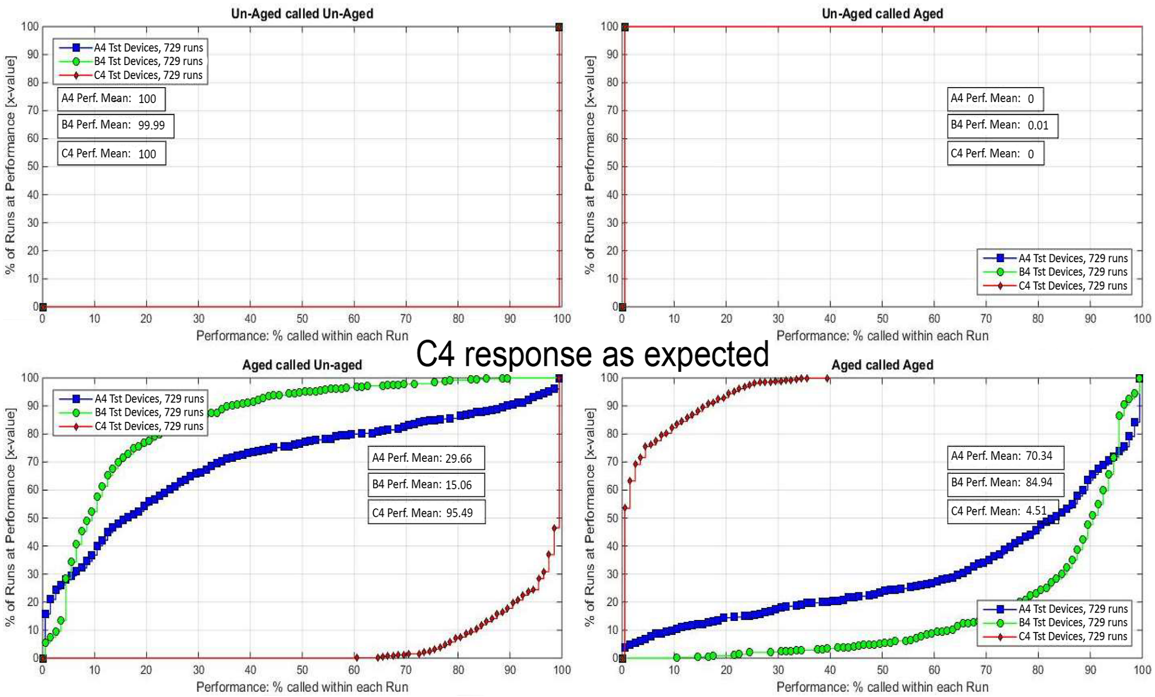


Figure 4.41. A4-B4-C4 Control Device CDFs. Includes 729 Runs (9 choose 3, with replacement) with all nine ages. C4 behaves as expected. A4 and B4 display results indicative of aging that are not expected.

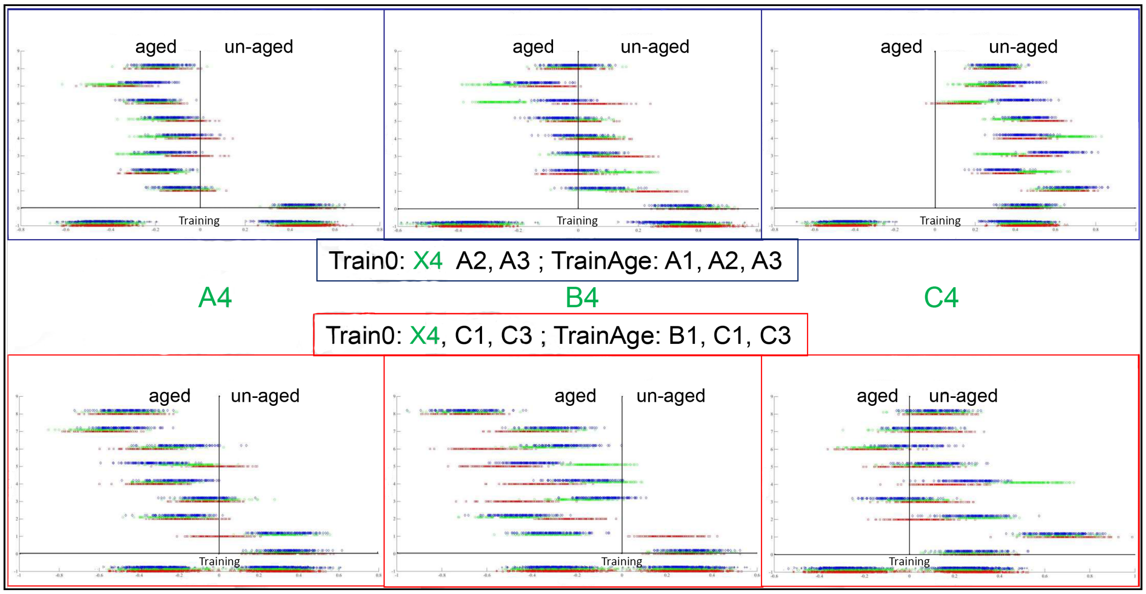


Figure 4.42. Control Device Repositioning Errors. C4 results for all ages (Age-0 to Age-8) remain centered on the Un-aged training mean as expected. A4 and B4 show a shift from Un-aged to Aged training means as the use fingerprint clusters on the Y-axis increase from Age-0 to Age-8.

In both training cases a clear shift occurs between the Age-0 and Age-1 to Age-8 fingerprints for both A4 and B4. This observed shift is not a function of positioning and the shift crosses the Un-Age to Age classification boundary. The fingerprint projections for C4 appear to stay centered on the Un-Aged training class cluster. These results indicate A4 and B4 truly demonstrate Aged (or at least different than Age-0) fingerprints. It is possible the month of run time imparted some wear-out attributes to A4 and B4 that are detected in this *Age Discrimination* procedure. However, C4 was in resting operational status just like A4 and B4 yet does not show any wear-out results.

Figure 4.42 only displays results for two training instances and was included to show the different A4 and B4 response are not likely due to repositioning. The reposition clusters for each age do not result in clusters crossing the classification boundary and do not overcome the shift between the Age-0 and Age-1 to Age-8 positions in the MDA/ML hyperplane. Figure 4.43 shows the called aged results for each of the nine labeled ages (Age-0 to Age-8) for all 729 training cases. A4/B4 are consistently reported as Aged at the higher labeled age collections. Something is changing in the A4 and B4 devices that looks like wear-out despite the same operational time for device C4.

Only On for Collections: D1 & D2

D1 and D2 were include in the 1st device slot used for training Class-1 (Example D1, A2, B2). Since D1 and D2 were never oven aged and only powered on during signal collections, all subplots should indicate Un-aged results. All subplots in Figure 4.44 demonstrate the expected response trends, spikes or curves shifted to 100% when calling devices Un-aged and spikes or curves shifted to 0% for tests calling devices Aged.

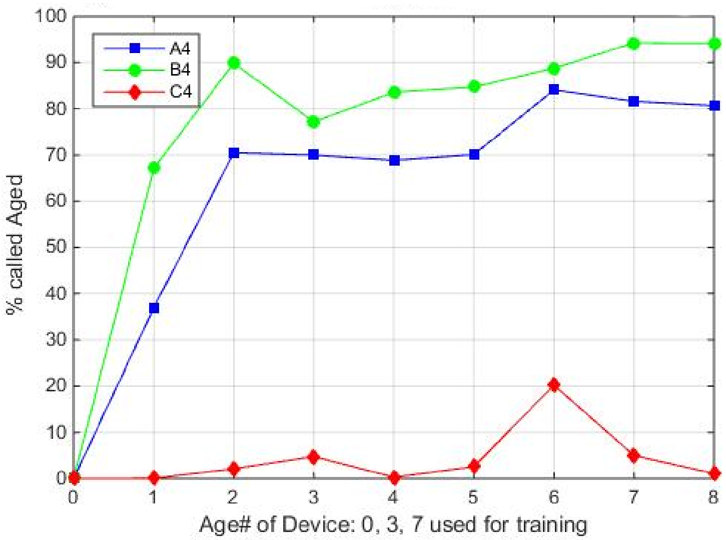


Figure 4.43. A4-B4-C4 Un-aged Control Device Called Aged Results. Training conducted with all 729 multi-device combinations and Control Device in 1st slot of Class-1. A4 and B4 results indicate aged phenomenon despite never being oven aged. As expected, C4 does not display aged phenomenon.

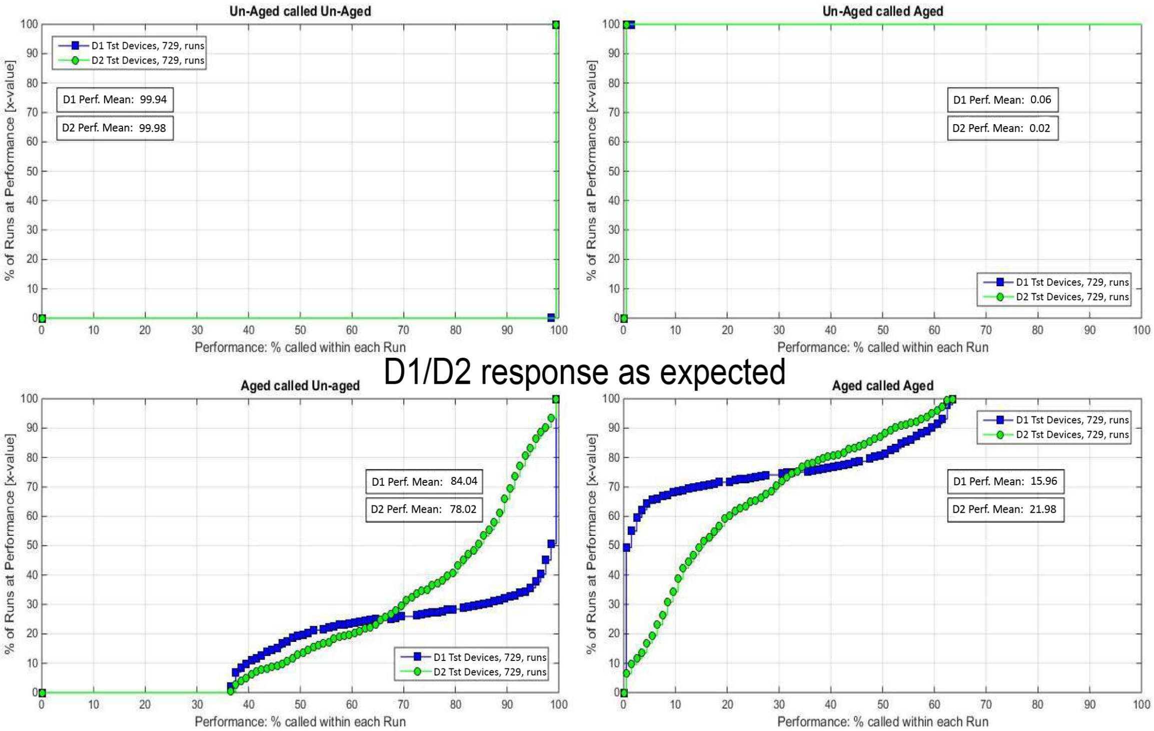


Figure 4.44. D1-D2 Control Device CDFs. Includes 729 Runs (9 choose 3, with replacement) with all nine Ages. Curves are as expected for Un-aged devices.

Burn-In: E1 & E2

E1 and E2 devices have no Un-Aged fingerprints. All labeled ages (Age-0, Age-1,...Age-8) include 100 hours of cumulative oven time. Therefore all three slots in Class-1 training remained as defined with the 729 device combinations with no changes to the Class-1 slot 1 position. All subplots in Figure 4.45 indicate the expected trends, spikes or curves shifted to 0% when calling devices Un-aged and spikes or curves shifted to 100% for tests calling devices Aged.

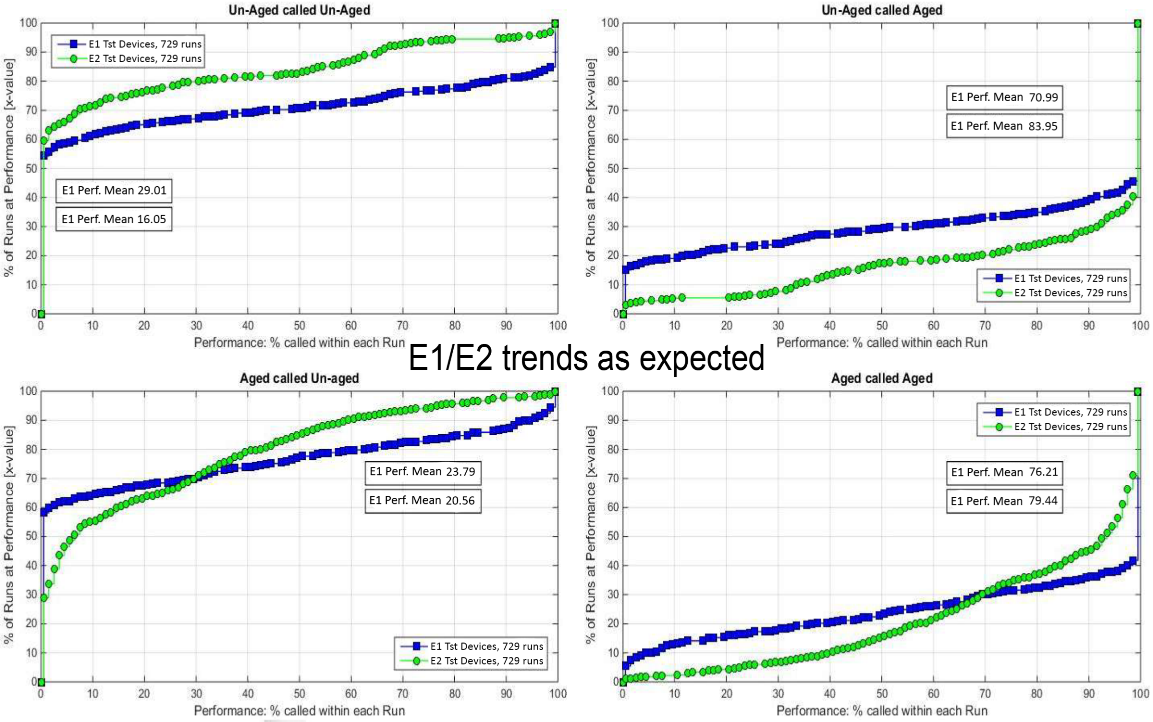


Figure 4.45. E1-E2 Control Device CDFs. Includes 729 Runs (9 choose 3, with replacement) with all nine Ages. Curves are as expected for Aged (Burn-in) devices.

V. Conclusion

This research addressed the proliferation of counterfeit electronic microelectronics and expanded the use for RF-DNA from previously studied application of Trojan/-modified hardware detection to the new application of identification of recycled components without intentional hardware modification. Electronic device wear-out was the physical phenomenon used to enable recycled component detection. Wear-out was imparted to the MSP-EXP430F5529LP micro-controller test devices by stressing operational devices with higher than manufacturer specified ambient temperature and recording signal emissions over a month of operation. The effect of wear-out on the previously examined hardware discrimination was also demonstrated.

The remainder of this chapter first highlights the research questions motivating this effort. The results of the three goals, *Device Discrimination*, *Aged Estimation*, and *Age Discrimination* are analyzed to answer the original questions. The results also manifested some challenges which reduced the accuracy of research results. Methods to improve this accuracy and further research suggestions are provide at the end of this chapter.

5.1 Research Questions

This section uses research results to answer the motivating questions:

1. *Device Discrimination*: Does transistor wear-out alter the accuracy of current URE RF-DNA device discrimination?

2. *Device Discrimination*: Do RF-DNA fingerprints have limited lifetimes; is sequential training needed to maintain accuracy?

3. *Device Discrimination*: Can the observation of device wear-out lead to an understanding of what mechanisms contribute to the device-to-device variations

in RF-DNA?

4. *Age Estimation*: Can RF-DNA estimate device age, how long a device has been in operation?
5. *Age Discrimination*: Can RF-DNA utilize wear-out changes in URE to identify aged (old/used) vs. un-aged (new/unused) devices?

5.1.1 *Device Discrimination*, Questions 1 - 3

Wear-out was demonstrated to impact *Device Discrimination* for the MSP430 devices and signal processing techniques utilized in this effort. The results imply RF-DNA training models have declining applicability over the course of a device's operational life for the devices considered in this effort. In the 2-Class comparisons the classification performance increased to an average performance of 93% when using models developed with incremental re-training from 78% accuracy when using the initial Age-0 discrimination model. The 3-Class comparisons produced a 31% performance gain from an average of 62% up to 93%.

The three incremental training ages showed better overall performance with the higher age training models. The overall results were generated by using testing fingerprints for all ages, Age-0 to Age-8, against the three incremental training ages: Age-0, Age-3 and Age-7. However, when looking at correct determination for the Age-0 fingerprints in isolation, the best results were produced by using the initial Age-0 training fingerprints, as seen in one example of Figure 3.31 in Section 3.3.2. This implies accurate determinations are age dependent and sequential training is needed depending upon the age at which peak accuracy is desired. Using the example of anti-tamper with an autonomous system from Section 1.2.1 the best accuracy for initial screening comes with training of initial Age-0 fingerprints. For anti-tamper testing at the one and two year points, best results should come with a one-year and two-year training set respectively. If limited to a single training set, training with fingerprints from a middle age provides the best average results across all ages.

The results obtained in this study utilized URE signals from devices that were intentionally stressed to impart wear-out variations. The accelerated aging techniques as well as signal filtering and subregion windowing targeting emissions around transistor state switching removed signal attributes that may remain constant over device operation. When attempting to improve device separation for *Age Estimation* efforts, the ratio of inter-class spread to intra-class spread was optimized with the wear-out optimized fingerprints (windowed sub-region signals). The fingerprints using non-windowed uniform subregions produced less separable classes but discrimination was still evident in the MDA/ML hyperplane with some class overlap. This result implies the features that give the best device discrimination with RF-DNA do indeed come from the uniqueness of transistor state switching be that static process variation from manufacturing (the idea enabling previous research hardware discrimination) or consumption of the design margin (the idea enabling this wear-out study).

5.1.2 *Age Estimation*, Question 4

Using the MDA/ML classifier, MSP430 micro-controllers and current RF-DNA techniques, Age Estimation was not attainable. Possible reasons for this outcome include:

1. Repositioning imparts variation that is on the same order, or greater than, the variation due to incremental wear-out.
2. MDA/ML class training separates classes equidistant from each other. For *Age Estimation*, the class separation needs to place higher age events at increasing distance from the un-aged class.

The range of projected cluster movement on the MDA hyperplane due to repositioning masked any trend in movement due to wear-out. Without a clear wear-out trend *Age Estimation* was not possible. While this original goal was not successful, attempts to reduce the impact of repositioning led to *Age Discrimination* success. It became evident when observing the projections on the MDA hyperplane, that a two-class age discrimination was possible since class wear-out age spread and reposition spread were typically both far removed from the Age-0 cluster on the 3-Class MDA hyperplane. After completion of the two-class *Age Discrimination* efforts, *Age Estimation* was not re-engaged due to the nature of MDA/ML classifier explained below.

The MDA/ML classifier maximizes all inter-class spread while simultaneously minimizing intra-class spread. In the case of the three-class (three age) training the resulting hyperplane places the three ages in roughly an equilateral triangle. This triangle results in all training class means spread by the same distance. To accomplish age estimation the spread between the min and max age needs to be larger than the spread between intermediate ages. Otherwise, another predictable monotonic measure mapping to age must be found. Even if repositioning did not impart distance variations on the order of class mean spread, the equal distant class mean separation would still prevent a monotonic regression line. The *Age Estimation* results and nature of MDA/ML classifier separation lead to the conclusion *RF-DNA application using MDA/ML is unable to conduct Age Estimation using the devices and techniques explored in this work.*

5.1.3 ***Age Discrimination*, Question 5**

URE RF-DNA was able to determine Un-Aged (new) vs. Aged (used) devices with average accuracy of 99.94% with an optimal test setup – testing devices matched with training devices. An intentional test setup forcing a worst case scenario, testing devices different from those used in training, still achieved 78.71% average accuracy. These results display two new assets of RF-DNA: 1) discrimination using attributes that are universal to all devices vs. individual device discrimination, and 2) application of RF-DNA to a population of devices using only a subset for training.

In the *Age Discrimination* tests, all hardware was designed to the same manufacturer specifications with no hardware alterations. Identical hardware along with MDA classifier training using multiple devices for each class definition (new vs. used) demonstrates that RF-DNA can identify URE features solely stemming from wear-out changes. With the classifier training finding globally applicable features across multiple devices the RF-DNA technique showed some success in identifying new vs. used devices that were never used for training. While these results were not perfect, this research indicates RF-DNA does not require a large training subset to apply models to a broader population of devices.

5.2 Accuracy Challenges: Repositioning

The need to incrementally oven-age devices and record URE signals at each increment required the removal and replacement of devices on the near-field signal collection testbed. This repositioning coupled with the fine beam-width of the Riscure near-field probe resulted in slight physical mis-alignments producing observable shifts in the MDA hyperplane.

These shifts produced some errors in all three research goals. The greatest impact was observed in *Age Estimation* and resulted in the inability to distinguish the shifts induced by repositioning from the desired incremental wear-out URE changes. *Device Discrimination* was also impacted with some instances of repositioning moving an entire repositioning subset of an age cluster across the classification boundary.

One such repositioning shift produced a 33% drop in accuracy for that age. Each age cluster included three repositioning subsets. Despite these errors the goal of observed age dependency in *Device Discrimination* was achieved. Reposition impacts in *Age Discrimination* were observable but minimized by training classes with multi-device fingerprints. Multiple device training resulted in wear-out variation dominating reposition errors producing less misclassification errors from repositioning.

5.3 Future Research Recommendations

Reducing Repositioning Errors

Means to eliminate or further reduce repositioning errors may improve the *Device Discrimination* and *Age Discrimination* results and enable *Age Estimation*. A URE alignment program similar to Stone's work [65] or a near-field probe with a wider beam-width may reduce repositioning errors. A wider beam-width probe could be implemented with the same Riscure probe used in this effort by raising the RF shield. In both cases, an alignment technique or wider beam-width, the goal is to reduce the percent error induced by not placing the main lobe of the RF-probe in the exact same location for each test device.

An improved position jig could reduce error by providing more consistent PCB placement. The jig used for this effort encompassed the entire perimeter of the PCB. In order to place the PCB into the jig, the aperture of the jig must be slightly larger than the PCB. Additionally, each PCB may have slightly different perimeters allowing additional space between the jig and PCB. Future work should consider position control by forcing a corner of the PCB into the corner of a two sided jig vs. encapsulating the entire PCB. Forcing the corners together would eliminate issues caused by PCB size tolerance variations.

Longer Aging - Device Failure

This initial work may be continued with longer aging profiles and carrying the wear-out to device failure. This work conducted limited aging and total run time was only carried out to one month; the 6-month Age-9 collections were deemed unusable. The ages used may only be at the beginning of the MSP430 operation lifetime and therefore only be at the beginning of the bathtub reliability curve. Aging devices to failure would allow for studies at the end of the bathtub curve. Work in this region could add the ability to identify eminent device failure in addition to the ability demonstrated in this work, namely to discriminate new vs. used components.

Targeted Hardware Wear-out

This effort used software implementing AES 128-bit encryption on the MSP430. Other options of software could explicitly exercise functional units on the MSP430 or other hardware in order to target specific areas of the IC die. The targeted hardware most prone to wear-out could increase age measurement accuracy. Additionally identifying locations prone to aging and other areas that are less susceptible could enable simultaneous age tracking and fingerprints that do not lose separability over device operational time.

Alternative Machine Learning

MDA/ML separates trained classes and makes a determination while comparing to all classes at the same time. Other machine learning techniques with a step-wise approach may produce success with the *Age Estimation* goal. For example, a cascade of binary decisions could identify a new vs. used items as done in this research, with a test producing an aged result. The next sequences could train a binary decision between two intermediate ages, with the test sequentially honing in on a best age.

5.4 Sponsor Acknowledgment

This research was sponsored in part by Air Force Research Laboratory / Sensors Directorate (AFRL/RY), Wright-Patterson AFB, OH.

Appendix A. AES Code

This attachment includes the C-code use to implement 128-bit AES encryption on the MSP430F5529 Evaluation boards. This code was obtained from the Texas Instruments website at:
http://www.ti.com/tool/AES-128?keyMatch=AES&tisearch=Search-EN-Everything

The code was modified to place a trigger signal and master clock on output pins and use Light Emitting Diode (LED) indicators on the evaluation board. Section A.1 - Main Loop contains the code main loop which calls the encryption code included in Section A.2 - AES Encrypt.

A.1 Main Loop

main_aes_loop.c

```
/* --COPYRIGHT--,BSD
 * Copyright (c) 2011, Texas Instruments Incorporated
 * All rights reserved. *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * *  Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * *  Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
```

```
* *  Neither the name of Texas Instruments Incorporated nor the names of
*    its contributors may be used to endorse or promote products derived
*    from this software without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
* AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
* THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
* CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
* EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
* PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
* OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
* WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
* OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
* EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
* --/COPYRIGHT--*/
#include <msp430.h>
#include "TI_aes_128_encr_only.h"

int main( void )
{
  WDTCTL = WDTPW + WDTHOLD;         // Stop watchdog timer

  P7SEL |= 0x80; // MCLK on pin 7.7
  P7DIR |= 0x80;

  P1DIR |= 0x01; P1OUT = 0x00; // Set P1.0 to output direction, Deppensmith mod for trigger
  P8DIR |= 0x06; P8OUT = 0x00; // Set P8.1 and P8.2 to output direction, Depp mod for error and loop count
             //8.1 (led2) for toggle of 500 loops, 8.2 (led3) for errors in one aes loop

  volatile unsigned int l; // volatile to prevent optimization, will use to count 500 loops
 l = 0;

  unsigned char err_count = 0;


  for(;;) { // Deppensmith mode for continual loop

  l=l+1;

  unsigned char i;

  unsigned char state[] = {0x00, 0x11, 0x22, 0x33, 0x44, 0x55, 0x66, 0x77,
                                 0x88, 0x99, 0xaa, 0xbb, 0xcc, 0xdd, 0xee, 0xff};
  unsigned char ciphertext[] = {0x69, 0xc4, 0xe0, 0xd8, 0x6a, 0x7b, 0x04,0x30,
                                  0xd8, 0xcd, 0xb7, 0x80, 0x70, 0xb4, 0xc5, 0x5a};
  unsigned char key[]   = {0x00, 0x01, 0x02, 0x03, 0x04, 0x05, 0x06, 0x07,
                             0x08, 0x09, 0x0a, 0x0b, 0x0c, 0x0d, 0x0e, 0x0f};

//  volatile unsigned int k; // volatile to prevent optimization
```

```
 P1OUT |= 0x01; // Set P1.0 high w/ OR to signal AES encrypt entry

  aes_encrypt(state,key);

  for (i=0;i<16;i++) {
   if (state[i] != ciphertext[i]) {
     err_count++;
   }
   if (err_count>0) {  //Deppensmith added to see if get errors
   P8OUT |= 0x04;  //led 3 on is an error, OR to preserve other LEDs
   //err_count=0;  //never reset so if err occurs in oven will alway be on
   }
 }

 if (l>=100) {
 l=0;
 P8OUT ^= 0x02;  //toggle led 2, when have 100 loops done
 err_count=0;
 P8OUT &= 0xFB;  //reset LED3 if it was on, keep LED2 in current state
 }
 }


 return 0;
}
```

A.2 AES Encrypt

TI_aes_128_encr_only.c

```
/* --COPYRIGHT--,BSD
 * Copyright (c) 2011, Texas Instruments Incorporated
 * All rights reserved.
 *
 * Redistribution and use in source and binary forms, with or without
 * modification, are permitted provided that the following conditions
 * are met:
 *
 * *  Redistributions of source code must retain the above copyright
 *    notice, this list of conditions and the following disclaimer.
 *
 * *  Redistributions in binary form must reproduce the above copyright
 *    notice, this list of conditions and the following disclaimer in the
 *    documentation and/or other materials provided with the distribution.
 *
 * *  Neither the name of Texas Instruments Incorporated nor the names of
 *    its contributors may be used to endorse or promote products derived
 *    from this software without specific prior written permission.
 *
 * THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS"
 * AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,
 * THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
 * PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR
 * CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL,
 * EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO,
 * PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS;
 * OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY,
 * WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR
 * OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE,
 * EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
 * --/COPYRIGHT--*/
/*
 * TI_aes_128_encr_only.c
 *
 *  Created on: Nov 3, 2011
 *      Author: Eric Peeters
 */


// foreward sbox
#include <msp430.h> //Depp added

const unsigned char sbox[256] =   {
//0     1    2      3     4    5     6     7      8    9     A      B      C     D     E     F
0x63, 0x7c, 0x77, 0x7b, 0xf2, 0x6b, 0x6f, 0xc5, 0x30, 0x01, 0x67, 0x2b, 0xfe, 0xd7, 0xab, 0x76, //0
0xca, 0x82, 0xc9, 0x7d, 0xfa, 0x59, 0x47, 0xf0, 0xad, 0xd4, 0xa2, 0xaf, 0x9c, 0xa4, 0x72, 0xc0, //1
0xb7, 0xfd, 0x93, 0x26, 0x36, 0x3f, 0xf7, 0xcc, 0x34, 0xa5, 0xe5, 0xf1, 0x71, 0xd8, 0x31, 0x15, //2
0x04, 0xc7, 0x23, 0xc3, 0x18, 0x96, 0x05, 0x9a, 0x07, 0x12, 0x80, 0xe2, 0xeb, 0x27, 0xb2, 0x75, //3
0x09, 0x83, 0x2c, 0x1a, 0x1b, 0x6e, 0x5a, 0xa0, 0x52, 0x3b, 0xd6, 0xb3,
0x29, 0xe3, 0x2f, 0x84, //4
0x53, 0xd1, 0x00, 0xed, 0x20, 0xfc, 0xb1, 0x5b, 0x6a, 0xcb, 0xbe, 0x39,
0x4a, 0x4c, 0x58, 0xcf, //5
0xd0, 0xef, 0xaa, 0xfb, 0x43, 0x4d, 0x33, 0x85, 0x45, 0xf9, 0x02, 0x7f,
0x50, 0x3c, 0x9f, 0xa8, //6
0x51, 0xa3, 0x40, 0x8f, 0x92, 0x9d, 0x38, 0xf5, 0xbc, 0xb6, 0xda, 0x21,
0x10, 0xff, 0xf3, 0xd2, //7
0xcd, 0x0c, 0x13, 0xec, 0x5f, 0x97, 0x44, 0x17, 0xc4, 0xa7, 0x7e, 0x3d,
0x64, 0x5d, 0x19, 0x73, //8
0x60, 0x81, 0x4f, 0xdc, 0x22, 0x2a, 0x90, 0x88, 0x46, 0xee, 0xb8, 0x14,
0xde, 0x5e, 0x0b, 0xdb, //9
0xe0, 0x32, 0x3a, 0x0a, 0x49, 0x06, 0x24, 0x5c, 0xc2, 0xd3, 0xac, 0x62,
0x91, 0x95, 0xe4, 0x79, //A
0xe7, 0xc8, 0x37, 0x6d, 0x8d, 0xd5, 0x4e, 0xa9, 0x6c, 0x56, 0xf4, 0xea,
0x65, 0x7a, 0xae, 0x08, //B
0xba, 0x78, 0x25, 0x2e, 0x1c, 0xa6, 0xb4, 0xc6, 0xe8, 0xdd, 0x74, 0x1f,
0x4b, 0xbd, 0x8b, 0x8a, //C
0x70, 0x3e, 0xb5, 0x66, 0x48, 0x03, 0xf6, 0x0e, 0x61, 0x35, 0x57, 0xb9,
0x86, 0xc1, 0x1d, 0x9e, //D
0xe1, 0xf8, 0x98, 0x11, 0x69, 0xd9, 0x8e, 0x94, 0x9b, 0x1e, 0x87, 0xe9,
0xce, 0x55, 0x28, 0xdf, //E
0x8c, 0xa1, 0x89, 0x0d, 0xbf, 0xe6, 0x42, 0x68, 0x41, 0x99, 0x2d, 0x0f,
0xb0, 0x54, 0xbb, 0x16 }; //F

// multiply by 2 in the galois field
unsigned char galois_mul2(unsigned char value)
{
 signed char temp;
```

```
  // cast to signed value
  temp = (signed char) value;
  // if MSB is 1, then this will signed extend and fill the temp variable with 1's
  temp = temp >> 7;
  // AND with the reduction variable
  temp = temp & 0x1b;
  // finally shift and reduce the value
  return ((value << 1)^temp);
}

// aes encryption function
// It manipulates the state and computes the key schedule on the fly
void aes_encrypt(unsigned char *state, unsigned char *key)
{
 unsigned char buf1, buf2, buf3, buf4, round, i;
 unsigned char rcon;

 // Rcon initial value. All subsequent values are computed.
 rcon = 0x01;

 // main AES data loop
 for (round = 0; round < 10; round++){
   if (round > 1) {
   P1OUT &= 0xFE; //Depp added reset P1.0 (trigger) low with AND on p1.0 set to go LOW
   }

```

```
//add key + sbox
   for (i = 0; i <16; i++){
     state[i]=sbox[state[i] ^ key[i]];
   }
   //shift rows
   buf1 = state[1];
   state[1] = state[5];
   state[5] = state[9];
   state[9] = state[13];
   state[13] = buf1;

   buf1 = state[2];
   buf2 = state[6];
   state[2] = state[10];
   state[6] = state[14];
   state[10] = buf1;
   state[14] = buf2;

   buf1 = state[15];
   state[15] = state[11];
   state[11] = state[7];
   state[7] = state[3];
   state[3] = buf1;

   //process mixcolumn for all rounds but the last one
   if (round < 9) {
     for (i=0; i <4; i++){
       // compute the current index
```

```
      buf4 = (i << 2);
buf1 = state[buf4] ^ state[buf4+1] ^ state[buf4+2] ^ state[buf4+3];
buf2 = state[buf4];
buf3 = state[buf4]^state[buf4+1]; buf3=galois_mul2(buf3); state[buf4] = state[buf4] ^ buf3 ^ buf1;
buf3 = state[buf4+1]^state[buf4+2]; buf3=galois_mul2(buf3); state[buf4+1] = state[buf4+1] ^ buf3 ^ buf1;
buf3 = state[buf4+2]^state[buf4+3]; buf3=galois_mul2(buf3); state[buf4+2] = state[buf4+2] ^ buf3 ^ buf1;
buf3 = state[buf4+3]^buf2;     buf3=galois_mul2(buf3); state[buf4+3] = state[buf4+3] ^ buf3 ^ buf1;
}
   }

   //key schedule
   // compute the 16 next round key bytes
   key[0] = sbox[key[13]]^key[0]^rcon;
   key[1] = sbox[key[14]]^key[1];
   key[2] = sbox[key[15]]^key[2];
   key[3] = sbox[key[12]]^key[3];
   for (i=4; i<16; i++) {
key[i] = key[i] ^ key[i-4];
   }
   // compute the next Rcon value
   rcon = galois_mul2(rcon);
 }

 // process last AddRoundKey
 for (i = 0; i <16; i++){
   state[i]=state[i] ^ key[i];
 }
}
```

Bibliography

1. Agarwal, M., Paul, B., Zhang, M. and Mitral, S. Circuit failure prediction and its application to transistor aging. *25th IEEE VLSI Test Symposium*, pages 277–286.

2. Alpaydin, Ethem. *Introduction to Machine Learning, 2nd Ed.* The MIT Press Cambridge, MA, USA, 2010.

3. Arasu, S., Nourani, M., Reddy, V. and Carulli, S. Controlling aging in timing-critical paths. *IEEE Design and Test*, 33(4):82–91.

4. Armstrong, Keith. What are the slew rates in digital circuits these days and what kinds of frequency spectra are generated? *The International Journal of Electromagnetic Compatibility*, Dec 2012.

5. Barnett, T., Singh, A., Grady, M. and Purdy, K. Yield-reliability modeling: Experimental verification and application to burn-in reduction. *VLSI Test Symposium, Proceeding 20th IEEE*, pages 75–80.

6. Boyer, A., Ndoye, A., Dhia, B., Guillot, L. and Vrignon, B. Characterization of the evolution of ic emissions after accelerated aging. *Electromagnetic Compatibility, IEEE Transactions on*, 51(4):892–900, 2009.

7. Carbino, T., Temple, M. and Bihl, T. Ethernet card discrimination using unintentional cable emissions and constellation-based fingerprinting. *Computing, Networking and Communications, International Conference on*, pages 369–373.

8. Carbino, T., Temple, M. and Lopez, J. Conditional constellation based-distinct native attribute (cb-dna) fingerprinting for network device authentication. *IEEE International Conference on Communications*, pages 1–6.

9. Cha, Ji Hwan. On optimal burn-in procedures – a generalized model. *IEEE Transactions on Reliability*, 55(2):198 – 206, Jun 2005.

10. Changlin, W., Jianmin, W., Xiangfeng, P., Fei, D. and Daojie, Y. Modelling and analysis of electromagnetic interferences for a 32-bit digital signal controller. *Antennas, Propagation and EM Theory (ISAPE), 2012 10th International Symposium on*, pages 1132–1135, 2012.

11. Cobb, W., Garcia, E., Temple, M., Baldwin, R. and Kim, Y. Physical layer identification of embedded devices using rf-dna fingerprinting. *Military Communications Conference, 2010 - MILCOM 2010*, pages 2168–2173, Nov 2010.

12. Cobb, W., Laspe, E., Baldwin, R., Temple, M. and Kim, Y. Intrinsic physical-layer authentication of integrated circuits. *Information Forensics and Security, IEEE Transactions on*, 7(1):14–24, 2012.

13. Cobb, W., Laspe, E., Baldwin, R., Temple, M. and Kim, Y. Intrinsic physical-layer authentication of integrated circuits. *Information Forensics and Security, IEEE Transactions on*, 7:1556–6013, Feb 2012.

14. Cobb, W., Temple, M., Baldwin, R. and Kim, Y. Physical layer identification of embedded devices using rf-dna fingerprinting. *Military Communications Conference, 2010 - MILCOM 2010*, 31(3):2168 –2173, Nov 2010.

15. Cobb, William. *Exploitation of Unintentional Information Leakage from Integrated Circuits*. Dissertation, Air Force Institute of Technology, Dec 2011.

16. DARPA. *TRUST for Integrated Circuits Proposal Solicitation: BAA06-40*. DARPA.

17. Defense Logistics Agency. *Department of Defense Test Method Standard: Microelectronics*. http://www.dscc.dla.mil/downloads/milspec/docs/mil-std-883/std883.pdf.

18. DeJean, G. and Kirovski, D. Rf-dna: Radio-frequency certificates of authenticity. *Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria*, 4727:346–363, 2007.

19. DiBene, J. and Knighten J. Effects of device variation on the emi potential of high speed digital integrated circuits. *Electromagnetic Compatibility, 1997. IEEE 1997 International Symposium on*, pages 208–212, 1997.

20. ENTech Electronics. Fr-4 pcb datasheet. Available at *www.entechelectronics.us/pdf/ILM%20GF212%20FR4.pdf*.

21. Ephraim, S. Aging-related failure rate obtained from bathtub curve data. *2015 IEEE Aerospace Conference*, pages 1–8.

22. Fang, J. and Sapatnekar, S. Incorporating hot-carrier injection effects into timing analysis for large circuits. *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, 22(12):2738–2751, 2014.

23. Ganta, D. and Nazhandali, L. Study of ic aging on ring oscillator physical unclonable functions. *15th International Symposium on Quality Electronic Design*, pages 461–467.

24. Getz, R. and Moeckel, B. Understanding and eliminating emi in microcontroller applications. Available at *www.ti.com/lit/an/snoa382/snoa382.pdf*.

25. Guin, U., Huang, K., DiMase, D., Carulli, J., Tehranipoor, M. and Makris, Y. Counterfeit integrated circuits: A rising threat in the global semiconductor supply chain. *Proceedings of the IEEE*, 102(8):1207–1228.

26. Guofujun, Zhoujiand and Xieronghua . The reliability approaches and requirements of ic component in telecom system. *Reliability Physics Symposium, 2012 IEEE International.*

27. Huang, K., Carulli, J., Makris, Y. Counterfeit electronics: A rising threat in the semiconductor manufacturing industry. *IEEE International Test Conference*, pages 1–4.

28. Huang, P., Wan, G. and Zhou, K. Improve effective capacity and lifetime of solid state drives. *Networking, Architecture and Storage (NAS), 2013 IEEE Eighth International Conference on*, 2013.

29. Ji, Z., Hatta, S., Zhang, J. F., et al. Negative bias temperature instability lifetime prediction: Problems and solutions. *Electron Devices Meeting (IEDM), 2013 IEEE International*, Dec 2013.

30. Keane, J., Wang, X., Persaud, D., and Kim, C. An all-in-one silicon odometer for separately monitoring hci, bti, and tddb. *IEEE Journal of Solid-State Circuits*, 45(4):817–829, April.

31. Khaleghi, S., Zhao, K., and Rao, W. Ic piracy prevention via design withholding and entanglement. *20th Asia and South Pacific Design Automation Conference*, pages 821–826.

32. Klein, R., Temple, M., Mendenhall, M. and Reising, D. Sensitivity analysis of burst detection and rf fingerprinting classification performance. In *IEEE International Conference on Communications, 2009. ICC '09.*, pages 1–5, june 2009.

33. Kohavi, R. and John, G. Wrappers for feature subset selection. *Artificial Intelligence*, pages 138–324, 1997.

34. Kohonen, T. Improved Versions of Learning Vector Quantization. *Neural Networks, 1990 IJCNN International Conference on*, pages 545–550, 1990.

35. Krishna, R. and Mal, A. Performance analysis of parallel adders in sub-micron and deep sub-micron technologies. *2016 International Conference on Microelectronics, Computing and Communications*, 2016.

36. Lim, T.C., Mulr, H., Finney, S.J. and Williams, B.E. Adaptive voltage slew control used to limit the magnitude of broadband conducted noise emissions fro buck derived dc-dc converters. *Electromagnetic Compatibility, 2012 Asia-Pacific Symposium on*, pages 93–96, May 2012.

37. Liu, Q. and Sapatnekar, S. Capturing post-silicon variations using a representative critical path. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 29(2):211–222, 2010.

38. Luo, H., Chen, X., Velamala, J., et al. Circuit-level delay modeling considering both tddb and nbti. *Quality Electronic Design (ISQED), 2011 12th International Symposium on*, pages 1–8, Mar 2011.

39. Maes, R. and Tuyls, P. *Secure Integrated Circuits and Systems.* Springer, 2010.

40. Mande, S., Chandorkar, A. and Iwai, H. Computationally efficient methodology for statistical characterization and yield estimation due to inter- and intra-die process variations. *Quality Electronic Design (ASQED), 2013 5th Asia Symposium on*, 2013.

41. Mazloum-Nejadari, A., Khatibi, G., Czerny, B., Lederer, M., Nicolics, J. and Weiss, L. Reliability analysis of cu wire bonds in microelectronic packages. *Thermal, Mechanical and Multi-physics Simulation and Experiments in Microelectronics and Microsystems, 2016 17th International Conference on*, pages 1–8.

42. Mendenhall, M., and Merenyi, E. Relevance-based feature extraction for hyperspectral images. *Neural Networks, IEEE Transaction on*, (4):648–672, April 2008.

43. MOSIS. *BSIM3v3.1 Model: Parameters extraction and optimization.* USC-ISI: The MOSIS Service. Available at
www.mosis.com/files/faqs/tech/bsim3.pdf.

44. MOSIS. *Reliability in CMOS IC Design: Physical Failure Mechanisms and their Modeling.* MOSIS: Metal Oxide Semiconductor Implementation Service. Available at
http://www.mosis.com/files/faqs/tech_cmos_rel.pdf.

45. NASA EEE Parts Assurance Group. *EE Parts Bulletin*, June 2011. Available at
https://nepp.nasa.gov/files/20647/2011%20EEE%20Parts%20Bulletin %20MayJune11%206_22_11.pdf.

46. Oppenheim, Alan V. and Schafer, Ronald W. *Discrete-Time Signal Processing.* Prentice Hall Press, Upper Saddle River, NJ, USA, 3rd edition, 2009.

47. Ordas, T., Lisart, M., Sicard, E., Maurine, P. and Torres, L. Near-field mapping system to scan in time domain the magnetic emissions of integrated circuits. *Integrated Circuit and Systems Design: Power and Timing Modeling, Optimization and Simulation. Volume 5349 of Lecture Notes in Computer Science*, pages 229–236.

48. Paul, B., Kunhyuk, K., Kufluoglu, H., Alam, M. and Roy, K. Impact of nbti on temporal performance degradation of digital circuits. *Electron Device Letters, IEEE*, 26(8):560–562, 2005.

49. Pawlikiewicz, A. and Elrai, S. Rf cmos or sige bicmos in rf and mixed signal circuit design. *14th International Conference on Mixed Design of Integrated Circuits and Systems*, pages 333–338, 2007.

50. Pey, K. L., Raghavan, N., Li, X., Liu, W. H., Shubhakar, K., Wu, X. and Bosman, M. New insight into the tddb and post breakdown reliability of novel high- gate dielectric stacks. *Reliability Physics Symposium (IRPS), 2010 IEEE International*, pages 354–363, May 2010.

51. Rahman, M. T., Forte, D., Shi, G., Contreras, G. and Tehranipoor, M. Csst: Preventing distribution of unlicensed and rejected ics by untrusted foundry and assembly. *Defect Tolerance in VLSI and Nonotechnology Systems, 2014 Internation Symposium on*, pages 46–51.

52. Riscure. *Inspector - the side channel test platform.* from http://www.riscure.com/inspector/product-description.html.

53. Saluja K., Vijayakumar, S., Sootkaneung, W. and Yang X. Nbti degradation: a problem or a scare? *VLSID 2008. 21st International Conference on*, pages 137–142, Jan 2008.

54. Samuel, S. and Temple, M. Rf-based anomaly detection for plcs in critical infrastructure applications. *International Journal of Critical Infrastructure Protection*, 5(2):11–33, Jul 2012.

55. Sandborn, P. *Cost Analysis of Electronic Systems.* World Scientific Publishing Company, Singapore, Nov 2012.

56. Sartori, J., Pant, A. and Kumar, R. Variation-aware speed binning of multicore processors. *Quality Electronic Design (ISQED), 2010 11th International Symposium on*, pages 307–314, 2010.

57. Shafiee, M., and Zuo, M. J. Optimising burn-in procedure and warranty policy in lifecycle costing, June 2011.

58. Shi, J., He, J., Chan, E., Slattery, K., Zhao, J., Fejfar, J. and Zanella, F. Equivalent radiation source extraction method for system level emi and rfi prediction. *Electromagnetic Compatibility, 2008. International Symposium on*, pages 1–5, 2008.

59. Skudlarek, J., Katsioulas, T. and Chen, M. A platform solution for secure supply-chain and chip life-cycle management. *Computer*, 49(8):28–34.

60. Steinecke, T. Microcontroller emission simulation based on power consumption and clock system. *Electromagnetic Compatibility of Integrated Circuits (EMC Compo), 2031 9th Intl Workshop on*, 2013.

61. Steinecke, T., Hesidenz, D. and Miersch, E. Emi modeling and simulation in the ic design process. *Electromagnetic Compatibility, 2006. International Zurich Symposium on*, pages 594–597, 2006.

62. Stone, B. and Stone, S. Comparison of radio frequency based techniques for device discrimination and operation identification. *Cyber Warfare and Security, International Conference on*, pages 475–484, Mar.

63. Stone, B. and Stone, S. Radio frequency based reverse engineering of microcontroller program execution. *National Aerospace and Electronics Conference*, pages 817–829, June.

64. Stone, S., Temple, M. and Baldwin, R. Detecting anomalous programmable logic controller behavior using rf-based hilbert transform features and a correlation-based verification process. *International Journal of Critical Infrastructure Protection*, 9(C):41–51, June.

65. Stone, Samuel J. *Radio Frequency Based Programmable Logic Controller Anomaly Detection*. PhD thesis, Air Force Institute of Technology, 2013.

66. Tai, K. and Kitakami, M. Prolongation of lifetime and the evaluation method of dependable ssd. *2010 IEEE 25th International Symposium on Defect and Fault Tolerance in VLSI Systems*, 2010.

67. Takahashi, E., Nakayama, T. and Saito, Y. Evaluation of packages by simulating ic emission using a leccs model, Feb 2006.

68. Tan, S., Yu, R. and Wan, S. Cost-effectively improving life endurance of mlc nand flash ssds via hierarchical data redundancy and heterogeneous flash memory. *Networking, Architecture and Storage (NAS), 2015 IEEE International Conference on*, 2015.

69. Texas Instruments. Mixed signal microcontroller datasheet. Available at *www.ti.com/lit/ds/symlink/msp430f5529.pdf*.

70. UC Berkeley Device Group. *BSIM Group*, 2012. Available at *www-device.eecs.berkeley.edu/bsim/?page=BSIM3*.

71. United States Government Accountability Office. *Counterfeit Parts*, Feb 2016. Available at *www.gao.gov/assets/680/675227.pdf*.

72. US Senate. *Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, Technical Report*. Committee on Armed Services.

73. Vattikonda, R., Wang, W. and Cao, Y. Modeling and minimization of pmos nbti effect for robust nanometer design. *Design Automation Conference, 2006 43rd ACM/IEEE*, pages 1047–1052, 2006.

74. Wang, X., Keane, J., Kim, T., Jain, P., Tang, Q. and Kim, C. Silicon odometers: compact in-situ aging sensors for robust system design. *IEEE Micro*, 34(6):74–85, Jan 2014.

75. Weste, N. and Harris, D. M. *CMOS VLSI Design: A Circuit and Systems Perspective, 4th Ed.* Addison-Wesley Boston, MA, USA, 2011.

76. Williams, M., Temple, M. and Reising, D. Augmenting bit-level network security using physical layer rf-dna fingerprinting. In *GLOBECOM 2010, 2010 IEEE Global Telecommunications Conference*, pages 1 –6, dec. 2010.

77. Wright, A., Hutzler, A., Schletz, A. and Pichler, P. Thermo-mechanical simulation of plastic deformation during temperature cycling of bond wires for power electronic modules. *Thermal, Mechanical and Multi-physics Simulation and Experiments in Microelectronics and Microsystems, 2014 15th International Conference on*, pages 1–5.

78. Wright, P. and Fan,M. A dfm methodology to evaluate the impact of lithography conditions on the speed of critical paths in a vlsi circuit. In *Proceedings of the 7th International Symposium on Quality Electronic Design*, 2006.

79. Xiaojun, L., Huang, B., Zhang, X. and Bernstein, J. A new spice reliability simulation method for deep submicrometer cmos vlsi circuits. *IEEE Transactions on Device and Materials Reliability*, 6(2):247–257, June.

80. Ye, Z. S., Tang, L. D. and Xie, M. Performance-based burn-in for products sold with warranty. *Industrial Engineering and Engineering Management (IEEM), 2011 IEEE International Conference on*, pages 1544 – 1548, Dec 2011.

81. Zeng, J., Abadir, M., Vandling, D., Wang, L., Karako, S. and Abraham, J. On correlating structural tests with functional tests for speed binning of high performance design. *Microprocessor Test and Verification (MTV'04), Fifth International Workshop on*, pages 103–109, 2004.

82. Zhang, X. and Tehranipoor, M. Design of on-chip lightweight sensors for effective detection of recycled ics. *IEEE Transactions on Very Large Scale Integration Systems*, 22(5):1016–1029, May.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)* 22–12–2016	**2. REPORT TYPE** Doctoral Dissertation	**3. DATES COVERED** *(From — To)* Sept 2013 - Dec 2016

4. TITLE AND SUBTITLE

Integrated Circuit Wear-out Prediction and Recycling Detection using Radio-Frequency Distinct Native Attribute Features

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Deppensmith, Randall D., Lieutenant Colonel, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-DS-16-D-002

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Research Laboratory, Integrated Electronic & Net-Centric Warfare Div
Attn: Yong C. Kim
2241 Avionics Circle
WPAFB OH 45433-7322
DSN 7981-8062, COMM 937-528-8026
Email: yong.kim@us.af.mil

10. SPONSOR/MONITOR'S ACRONYM(S)

AFRL/RYWA

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

14. ABSTRACT

Radio Frequency Distinct Native Attribute (RF-DNA) has shown promise for detecting differences in Integrated Circuits (IC) using features extracted from a device's Unintentional Radio Emissions (URE). This ability of RF-DNA relies upon process variation imparted to a semiconductor device during manufacturing. However, internal components in modern ICs electronically age and wear out over their operational lifetime. RF-DNA techniques are adopted from prior work and applied to MSP430 URE to address the following research goals: 1) Does device wear-out impact RF-DNA device discriminability?, 2) Can device age be continuously estimated by monitoring changes in RF-DNA features?, and 3) Can device age state (e.g., new vs. used) be reliably estimated? Conclusions include: 1) device wear-out does impact RF-DNA, with up to a 16% change in discriminability over the range of accelerated ages considered, 2) continuous (hour-by-hour) age estimation was most challenging and generally not supported, and 3) binary new vs. used age estimation was successful with 78.7% to 99.9% average discriminability for all device-age combinations considered.

15. SUBJECT TERMS

RF-DNA, Transistor Wear-out, Accelerated Aging, Physical Layer Cyber-security, Integrated Circuit Lifetime, Counterfeit / Recycled IC Detection

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Dr. Michael Temple (AFIT/ENG)
U	U	U	U	142	**19b. TELEPHONE NUMBER** *(include area code)* (937) 255-3636, x4279; michael.temple@afit.edu